WEST

Help | Logout | Interrupt

Main Menu | Search Form | Posting Counts | Show S Numbers | Edit S Numbers | Preferences | Cases

Search Results -

Term	Documents
NOTIFICATION	18575
NOTIFICATIONS	2562
(4 AND NOTIFICATION).USPT.	2
(L4 AND (NOTIFICATION)).USPT.	2

Database: US Patents Full-Text Database
US Pre-Grant Publication Full-Text Database
JPO Abstracts Database
EPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L6

Refine Search

Recall Text | Clear

Search History

DATE: Thursday, September 11, 2003 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT; PLUR=YES; OP=OR			
L6	l4 and (notification)	2	L6
L5	l4 and (message near notification)	0	L5
L4	L3 and spammer$	8	L4
L3	L2 and ((unwant$ or unsolicit$ or spam$) near email)	26	L3
L2	(electronic near mail) or email	8378	L2
L1	(electronic near mail) oe email	739834	L1

END OF SEARCH HISTORY

L6: Entry 1 of 2 File: USPT Apr 2, 2002

DOCUMENT-IDENTIFIER: US 6366950 B1
TITLE: System and method for verifying users' identity in a network using e-mail communication

Brief Summary Text (12):
In addition to these security concerns, a further concern is that users can camouflage their real identity, for example, by regularly changing the screen name and/or their return address in an electronic mail message (email).

Brief Summary Text (16):
An aspect of the invention involves a method of maintaining a user identification database that indicates when users are in communication with a network. The method includes the acts of associating in a computer accessible storage medium, electronic mail addresses, processor-embedded identifiers and status information. A first electronic message is received from a first computer. The first electronic message contains an electronic mail address and a copy of the processor-embedded identifier existing in the first computer. The first electronic mail address is used to access the corresponding processor-embedded identifier stored in the storage medium. The processor-embedded identifier from the first computer is compared with the processor-embedded identifiers of the storage medium. The status information in the storage medium is modified to indicate that the first electronic mail address is authentic when the processor-embedded identifier from the first computer matches a processor-embedded identifier of storage medium.

Detailed Description Text (10):
The communications modules, for example, allows communications between the computers 2, 4 in accordance with preferable standardized communications protocols. In one typical application, the communications protocols support the exchange of emails. These communications protocols include a Transmission Control Protocol/Internet Protocol (TCP/IP), a Simple Mail Transfer Protocol (SMTP), a File Transfer protocol (FTP), a Hypertext Transfer Protocol (HTTP) and a Lightweight Directory Access Protocol (LDAP).

Detailed Description Text (11):
The TCP/IP is a protocol that specifies how computers exchange data over the Internet, The TCP/IP handles tasks such as packetization, packet addressing, handshaking and error correction. The SMTP is used to transfer email between computers. Generally, the SMTP is a server-to-server protocol, so other protocols are used to access the messages. The SMTP dialog usually happens in the background under the control of a message transport system. The FTP is a client-server protocol that allows a user on one computer to transfer files to and from another computer over a TCP/IP network. The ITTP is a client-server TCP/IP protocol used on the World-Wide Web for the exchange of HTML documents. The LDAP is a relatively simple protocol for updating and searching directories running over TCP/IP, as described below in greater detail.

Detailed Description Text (13):
Computers can communicate with each other, for example, over the Internet, because each computer can be addressed individually. In such embodiments, certain computers have an assigned Internet protocol address (IP address). The IP address is a 32-bit host address that is usually represented in dotted decimal notation, for example, 128.121.4.5. The decimal IP address is in most cases not known to the user. In addition, most users are not aware that this IP address exists. In addition, in many embodiments, a computer user has an assigned email address that specifies the source or destination of the message. The email address is typically in the form of "name@xyz.com", for example, as known in the art.

Detailed Description Text (14):

In accordance with one embodiment of the present invention, the ID number serves to address, identify and authorize computers. As mentioned above, the ID number is unique to a computer and cannot be altered. This provides a higher degree of reliability and security, because the IP address and the email address can be altered. For instance, some users alter the email address or the address field to camouflage the return address and, thus, their real identity.

Detailed Description Text (15):
Returning to the embodiment illustrated in FIG. 1. The user of the computer 2 writes an email to be sent to the user of the computer 4. When the email is composed and the user initiates transmission to the computer 4 over the communications medium 6, the communications software (e.g., SMTP) automatically converts the email into an appropriate electronic data format. Besides the actual email message, the return email address and the return IP address, the data format includes, in accordance with the present invention, the microprocessor-specific ID number.

Detailed Description Text (16):
The computer 4 receives the electronic representation of the email and converts it back to a user-readable message. During the process of converting, the computer 4 extracts the received ID number and compares (looks-up) it with the ID number(s) stored in the data base 7. When the received ID number matches one of the stored ID numbers, the computer 4 accepts the email as one received from an authorized computer.

Detailed Description Text (17):
The look-up of the ID number is generally triggered by an event. That is, when the computer 4 receives the email message, the look-up procedure starts. It is contemplated that the user of the computer 4 can define the specifics of the event-triggered look-up. For instance, the user can define if a notification of the requested look-up shall occur or if a recording or display of the look-up is desired.

Detailed Description Text (18):
The user of the computer 4 can define how emails from computers whose ID numbers are not stored in the database need to be treated. Depending on user-specified settings of the computer 4, emails from unauthorized/unidentified computers can be, for example, blocked or rejected. For instance, the user can create a contact list in which all authorized users are listed. If the received ID number does not match to the ID number stored for an authorized user from the contact list, the email will be rejected.

Detailed Description Text (19):
These settings, for example, prevent the user from receiving undesired emails from individuals who frequently change their email address or camouflage the return address. These undesired emails cannot be blocked by conventional filters which can be defined in email applications because the filters are typically only sensitive to the field "From:" for the return address.

Detailed Description Text (20):
In addition, the settings prevent the user from receiving unsolicited emails from Internet marketing companies or so-called "spammers." A "spammer" is an individual user or a service which post irrelevant or inappropriate messages to one or more users, send large amounts of unsolicited emails meant to promote a product or service, or intend to crash a program by overrunning a fixed-size buffer with excessively large input data.

Detailed Description Text (21):
Moreover, the computer 4 cannot only block or reject emails from unauthorized users, but also identify if the return email address that appears in the field "From:" is indeed the real email address. For example, the sender of the email could pretend to be an authorized user by changing the email address to one the sender believes the computer 4 accepts. However, because the ID number is included to the received email, the false identity of the sender of the email can be recognized.

Detailed Description Text (39):
FIG. 3 shows an exemplary data format as used in the identification database 32. The identification database 32 includes several fields 32A-32F of predetermined sizes. Each field 32A-32F includes an attribute. In the illustrated embodiment, the ID number is assigned to the field 32A which has a size of 44 bits. The user name and the email address are assigned to the fields 32B, 32D, respectively. The field 32B has a size of 128 bits and the field 32D has a size of 256 bits. The field 32C includes an attribute "activity status" and the field 32E includes an attribute "authentication statues." The field 32F includes an attribute "ISP" defining the Internet service provider. It is

contemplated that the identification database 32 can include additional fields, such as for the IP address, geographical data and other user information.

Detailed Description Text (40):
In one embodiment, only the email address and the ID number are indexed. As is known in the art, an index is a sequence of (key pointer) pairs where each pointer points to a record in the database that contains the key value in a particular field. The index is sorted on the key values to allow rapid searching for a particular key value. In one embodiment, the index can be "inverted" in the sense that the key value is used to find the record rather than the other way round. For databases in which the records may be searched based on more than one field, multiple indices may be created that are sorted on those keys.

Detailed Description Text (42):
The client module 28 prompts the user to input the email address. The user inputs the email address under which the user can receive emails. During a subroutine in state 202, the client module 28 retrieves the ID number from the processor and prepares a message to be sent to the server 26. The client module 28 includes as a default setting, the IP address of the server 26. In addition, the client module 28 may have a list of additional appropriate servers connected to the Internet 24.

Detailed Description Text (44):
Upon connection to the, Internet service provider, the procedure proceeds along the YES branch to state 208. In state 208, the client module 28 (e.g., via SMTP) initiates that the prepared message is sent to the server 26. The message includes the ID number, the user's email address and the IP address. It is contemplated that additional information can be added depending on the data format used, as described below with reference to FIG. 5.

Detailed Description Text (52):
In one example, the users of the computers 20, 22 have both registered with the server 26 through the procedure illustrated in FIG. 4. In addition, the computers 20, 22 defined contact lists so that the computers 20, 22 accept only emails from authorized computers.

Detailed Description Text (56):
Proceeding to state 304, the user of the computer 20, or any other registered computer, can request a look-up of an email address from the server 26. Here, the user requests a look-up of the email address of the user of the computer 22. The user of the computer 20 prepares a message (email) to the server requesting the look-up of the email address included in the message. The message is sent over the Internet 24 to the server 26.

Detailed Description Text (57):
Proceeding to state 306, the server 26 receives the message from the Internet 24 ad initiates processing the message. The processing includes starting a module to look-up the email address in the identification database 32. The subroutine uses known methods to access and retrieve data from a database. The subroutine extracts the look-up email from the received message and checks if the identification database 32 includes a matching entry.

Detailed Description Text (58):
Proceeding to state 308, the server 26 generates a second message that is a response to the first message received from the computer 20. If the look-up did not result in a matching address, the second message informs the user of the computer 20 that no matching entry has been found. If, however, the look-up was successful, the second message includes an authenticated email address, authenticated because the email address is correlated to the unique ID number. In addition, the second message can include data indicating, for example, if the computer 22 is currently registered as active, i.e., if the user of the computer 22 is online at the moment.

Detailed Description Text (59):
Proceeding to state 310, the computer 20 receives the second message and extracts the authenticated email address of the computer 22. As in a conventional email application, the user of the computer 20 can read the email upon receipt or at a later time.

Detailed Description Text (60):
Proceeding to state 312, the user of the computer 20 can directly communicate with the user of the computer 22 using the authentic email address. To communicate, the user of the computer 20 has several options. The user can send an email to the user of the

computer 22 that will be recognized as coming from a known contact. Alternatively, the user can connect directly to the computer 22 to initiate an online conferencing connection, such as a chat connection, a video conference, or a voice connection, if the user of the computer 22 is currently online or available. The procedure ends at state 314.

Detailed Description Text (61):
The described look-up via email address is typically the only way for users to find one another. This makes the system a closed system and attractive to users who do not want their information published. In particular, the system provides improved security and confidentiality for transactions that involve financial or personal data.

Detailed Description Text (67):
As soon as the user USER-1 is online, the client module 50 API (SDK) automatically sends a message to the server 26, as indicated through a connection line L1. The message includes the ID number. The message may also include, but is not limited to, the IP address and email address as described above. The directory module 74 receives and processes the message and initiates an update of the identification database 32. The user USER-1 is then stored as an active user.

Detailed Description Text (68):
If the user USER-i wants to communicate with the Internet service provider ISP-1, the user USER-1 requests a look-up of the email address of the Internet service provider ISP-1. The server 26 executes this look-up request and generates a response if the requested email address matches one of the stored and authenticated email addresses. The generated response includes the IP address of the Internet service provider ISP-1. The response sent to the user USER-1 is indicated through a connection line L2. Using the IP address, the user USER-1 can then directly connect to the Internet service provider ISP-1.

Detailed Description Text (70):
If the user USER-2 requests a look-up of the email address of the user USER-3, the response includes the IP address of the computer 44 of the user USER-3. The user USER-2 can then directly connect to the user USER-3 to send an email, to chat, to have a video conference, or the like. The connection between the computers 42, 44 is indicated as connection line L8.

Detailed Description Text (71):
It is contemplated that the user USER-2 can look-up a variety of email addresses. A general connection with a computer connected to the Internet 24 is indicated through a connection line L9. Correspondingly, the user USER-3 can connect to the Internet service provider ISP-2 via the Internet 24, as indicated through a connection line L1 . Alternatively, the computer 22 and the service computer can be connected through the communications link 60, as described above.

Detailed Description Text (76):
In this example, the web computer 80 and the client computer 84 have registered with the server 26 according to the registration procedure illustrated in FIG. 4. Using a communications link C1, the user of the client computer 84 requests a look-up of the email address of the Internet shop. The server 26 performs the look-up in its database 92 and returns an authenticated email address if the look-up email address matches to an entry correlated to the ID number in the database 92.

Detailed Description Text (77):
The user of the client computer 84 can then establish a direct communications link C2 with the web computer 80 using the authenticated email address. This assures the user of the client computer 84 that the communication occurs directly with the Internet shop when the user places an order with the Internet shop. In some cases, the Internet shop requires that the order include consumer-specific data such as name, address and the number of the credit card.

Detailed Description Text (78):
Before the Internet shop confirms the order via a communications link C3, the Internet shop can request a look-up of the client's email address to ensure that the data of the order is correct. The look-up request and the resulting response occur via communications links C4, C5, respectively.

Detailed Description Text (79):
As described above, the ID numbers are unique within the identification database 32 as

well as within the Internet 24. In contrast, user names and email addresses, for example, can appear more than once within continuously growing global Internet. Because of this, there may be two users that claim to have the same email address. If such a collision occurs on a lookup, both users will be returned from the query. The identification database 32 permits users to look up other users only by email address and not by the ID number. However, the index to the ID number is there, because the contact list may need to look up a specific ID number.

CLAIMS:

1. A method of maintaining a user identification database that indicates when users are in communication with a network, the method comprising the acts of:

associating in a computer accessible storage medium electronic mail addresses, processor-embedded identifiers and status information;

receiving a first electronic message from a first computer, the first electronic message containing an electronic mail address and a copy of the processor embedded identifier existing in the first computer;

using the first electronic mail address to access the corresponding processor-embedded identifier stored in the storage medium;

comparing the processor-embedded identifier from the first computer with the processor-embedded identifiers of the storage medium;

modifying the status information in the storage medium to indicate that the first electronic mail address is authentic when the processor-embedded identifier from the first computer matches a processor-embedded identifier of storage medium;

receiving a second electronic message from a second computer, the second electronic message requesting authentication of the first electronic mail address;

comparing the first electronic mail address with the electronic mail addresses stored in the storage medium; and

sending a third message to the second computer that indicates whether the first electronic mail address is authentic.

2. The method of claim 1, further comprising the acts of:

obtaining the status information that corresponds to the first electronic mail address; and

including the status information to the third message.

3. The method of claim 1, further comprising the act of using the authenticated first electronic mail address to establish a communications link between the first and second computers.

5. The method of claim 1, wherein the act of receiving the second electronic mail includes indicating the second computer as active in the storage medium.

6. The method of claim; 1, wherein the act of associating electronic mail addresses includes registering the first and second computers in a computer accessible database.

7. The method of claim 6, wherein the act of registering includes storing each processor-embedded identifier in the database together with the electronic mail address of the registering computer.

WEST

Generate Collection Print

L4: Entry 5 of 8 File: USPT Nov 20, 2001

DOCUMENT-IDENTIFIER: US 6321267 B1
TITLE: Method and apparatus for filtering junk email

Abstract Text (1):
An Active Filtering proxy filters electronic junk mail (also known as spam, bulk mail, or advertising) received at a Message Transfer Agent from remote Internet hosts using the Simple Mail Transfer Protocol (SMTP). The proxy actively probes remote hosts that attempt to send mail to the protected mail server in order to identify dialup PCs, open relays, and forged email. The system provides multiple layers of defense including: connect-time filtering based on IP address, identification of dialup PCs attempting to send mail, testing for permissive (open) relays, testing for validity of the sender's address, and message header filtering. A sender's message must successfully pass through all relevant layers, or it is rejected and logged. Subsequent filters feed IP addresses back to the IP filtering mechanism, so subsequent mail from the same host can be easily blocked.

Brief Summary Text (3):
This invention generally concerns electronic messaging. In particular, the present invention concerns a system for filtering undesired electronic mail.

Brief Summary Text (5):
Generally, the term "spam" has come to refer to posting electronic messages to news groups or mailing to addresses on an address list the same message an unacceptably large number (generally, 20-25) of times. As used herein, the term "spam" or "junk mail" refers to the sending of unsolicited electronic messages (or "email") to a large number of users on the Internet. This includes email advertisements, sometimes referred to as Unsolicited Commercial Email (UCE), as well as non-commercial bulk email that advocates some political or social position. A "spammer" is a person or organization that generates the junk mail.

Brief Summary Text (6):
The principal objection to junk mail is that it is theft of an organization's resources, such as time spent by employees to open each message, classify it (legitimate vs. junk), and delete the message. Time is also spent by employees following up on advertising content while on the job. In addition, there is an increased security risk from visiting web sites advertised in email messages. Employees may also be deceived into acting improperly, such as to release confidential information, due to a forged message. Still yet, there is a loss of the network administrator's time to deal with spam and forged messages, as well as the use of network bandwidth, disk space, and system memory required to store the message. Finally, in the process of deleting junk mail, users may inadvertently discard or overlook other important messages. Another objection to junk mail is that it is frequently used to advertise objectionable, fraudulent, or dangerous content, such as pornography, illegal pyramid schemes or to propagate financial scams.

Brief Summary Text (7):
Spam can also be a serious security problem. For instance, the recent Melissa virus and ExploreZip.worm have been spread almost exclusively via email attachments. Such viruses are usually dangerous only if the user opens the attachment that contains the malicious code, but many users open such attachments.

Brief Summary Text (8):
Email may also be used to download or activate dangerous code, such as Java applets, Javascript, and ActiveX controls. Email programs that support Hypertext Markup Language (HTML) can download malicious Java applets or scripts that execute with the mail user's privileges and permissions. Email has also been used to activate certain powerful

ActiveX controls that were distributed with certain operating systems and browsers. In this case, the code is already on the user's system, but is invoked in a way that is dangerous. For instance, this existing code can be invoked by an email message to install a computer virus, turn off security checking, or to read, modify, or delete any information on the user's disk drive.

Brief Summary Text (9):
Both spammers, and those who produce malicious code, typically attempt to hide their identities when they distribute mail or code. Instead of mailing directly from an easily-traced account at a major Internet provider, they may, for instance, send their mail from a spam-friendly network, using forged headers, and relay the message through intermediate hosts. Consequently, the same mechanisms that can be used to block spam can also be used to provide a layer of protection for keeping malicious code out of an organization's internal network.

Brief Summary Text (11):
Simple Mail Transfer Protocol (SMTP) is the predominant email protocol used on the Internet. It is a Transmission Control Protocol/Internet Protocol (TCP/IP) communication protocol that defines the message formats used for transfer of mail from one Message Transfer Agent (MTA) via the Internet to another MTA. As shown in FIG. 1, Internet mail operates at two distinct levels: the User Agent (UA) and the MTA. User Agent programs provide a human interface to the mail system and are concerned with sending, reading, editing, and saving email messages. Message Transfer Agents handle the details of sending email across the Internet.

Brief Summary Text (12):
According to SMTP, an email message is typically sent in the following manner. A user 1040 (located at a personal computer or a terminal device) runs a UA program 1041 to create an email message. When the User Agent completes processing of the message, it places the message text and control information in a queue 1042 of outgoing messages. This queue is typically implemented as a collection of files accessible to the MTA. In some instances, the message may be created on a personal computer and transferred to the queue using methods such as the Post Office Protocol (POP) or Interactive Mail Access Protocol (IMAP).

Brief Summary Text (16):
The sending host's Message Transfer Agent 1001 sends an email message to the receiving host 1002. At step 1010, the sending MTA opens a TCP connection to the receiving host's reserved SMTP port. This is shown as a dashed line with an italics description to differentiate it from the subsequent protocol messages. This typically involves making calls to the Domain Name System (DNS) to get the IP address of the destination host or the IP address from a Mail Exchange (MX) record for the domain. For example, the domain escom.com has a single MX record that lists the IP address 192.135.140.3. Other networks, particularly large Internet Service Providers (ISPs), might have multiple MX records that define a prioritized list of IP addresses to be used to send email to that domain.

Brief Summary Text (21):
At step 1014, the sending MTA sends a MAIL From: message to identify the email address of the sender of the message, e.g., sender@remote.dom. By convention, the Internet address is formed by concatenating the sending user's account name, the "@" sign, and the domain name of the sending host. The resulting address is typically enclosed in angle-brackets, however, this is not usually required by the receiving mail server. It is noted that spammers can easily forge the MAIL address.

Brief Summary Text (25):
When the sending MTA receives this reply, it sends the text of the email message one line at a time as shown in step 1020. Note that it does not wait for a response after each line during this phase of the protocol. The message includes the SMTP message header, the body of the message, and any attachments (perhaps encoded) if supported by the sending User Agent program.

Brief Summary Text (28):
The email message header is transferred at the beginning of the message and extends to the first blank line. It includes Received: lines added by each MTA that received the message, the message timestamp, message ID, To and From addresses, and the Subject of the message. The message header is followed by the body of the message (in this case, a single line of text), the terminating period, and the final handshaking at the end of the message. Here, the term "message" alone refers to the overall email message as well

as the multiple protocol messages (e.g., HELO, MAIL and RCPT) that are used by SMTP.

Brief Summary Text (29):
Spammer Techniques

Brief Summary Text (30):
The two primary techniques used by spammers are relaying and directing SMTP from a dialup PC. Approximately one-half of all spam attempts are relayed from an attacker through an intermediate site that permits relaying. Many of these open relay sites have been recently added to the Internet without regard to good system administration practices, and consequently may permit relaying without regard to its consequences.

Brief Summary Text (31):
Approximately one-third of junk mail is sent directly from a dialup PC to the recipient mailhost. The use of direct SMTP from a PC provides the ability to forge email. As open relays are closed, this percentage is likely to rise. The remainder (approximately 15%) of junk mail is from users that appear to have an account on the sending network.

Brief Summary Text (32):
Regardless of which technique is used, however, almost all junk mail have similar characteristics. Junk mail messages almost invariably have a forged email address in order to discourage complaints by the recipients of the spam. Contact information is provided somewhere in the body of the message, and may be another email address, a link to a web page or a telephone number. In addition, junk mail frequently does not include the recipient's address in the header of the message. This is done primarily as a performance optimization.

Brief Summary Text (33):
In addition, junk mail is usually sent from a "throwaway" account, in which the spammer sends a batch of messages (usually thousands of messages) and then moves on after being canceled. Similarly, spamming networks sometimes perform spam runs from a mail server, then take the host offline to avoid complaints. Such networks operate until they are widely blacklisted, then register a new domain and carry on business under a different name.

Brief Summary Text (34):
Any person with an email address at an Internet Service Provider (ISP) account can send junk email. After acquiring an address list, the user can send a message to each address on the list using the mailer program provided by the ISP. However, as shown in the examples in FIGS. 2 and 3, most ISPs record the sender's actual email address in outgoing message headers. If recipients complain, the ISP will often terminate the user's account, sometimes billing cleanup fees in accordance with the network's Acceptable Use Policy (AUP). Consequently, this technique is not favored by most spammers.

Brief Summary Text (38):
Open relays permit the spammer to easily forge his/her identity. FIG. 4 shows how a spammer at spam.dom 1060 relays mail via relay.dom 1061 to a variety of different users at different target domains 1062, 1074, etc. At step 1063, the spammer connects to relay.dom, as described with regard to FIG. 2. For clarity, SMTP responses (greeting messages, 250, etc.) are not shown in this figure.

Brief Summary Text (39):
At step 1064, the spammer forges a MAIL From message listing an address at the open relay host 1061. The forged MAIL address can be at any network, including spam.dom, relay.dom, any of the netn.dom hosts, or somewhere else. The forged MAIL From: address may be the same as the From: line in the message header, or it may be different. At one time spammers commonly forged addresses at AOL.COM or other large networks, because those networks were so well known, but legal action by AOL in particular has largely stopped that practice. The spammer is able to forge the MAIL address usually because he or she is able to override the normal user authentication functions, perhaps as a trusted user of a network server or as the operator of a single-user PC.

Brief Summary Text (40):
At steps 1065, 1066, the spammer sends multiple RCPT messages with a list of destination addresses. Finally, step 1068, the spammer sends a DATA message, the text of the email message, a period, and a quit message to relay.dom. When relay.dom receives the message, it stores the message in its mail queues until it has forwarded the message to each of the target addresses, or until the message has timed out. If it

cannot deliver a message, it will typically retry periodically (perhaps every 10 minutes or perhaps once per day). The relay host will usually keep undelivered messages in its queue for up to a week.

Brief Summary Text (42):
The difficulty in filtering relayed junk mail is shown in part by this example. If the spammer 1060 forges the MAIL From address to match the relay host (e.g., "good@relay.dom") then as observed by net1.dom 1062, the message appears to be from a legitimate user at relay.dom. This example shows abuse of one open relay. The current generation of relaying tools will also permit the spammer to enter a list of open relay hosts, and the software will use different relays for different groups of addresses. Thus, different users at the same target network may receive spam relayed via different paths.

Brief Summary Text (48):
FIG. 6 shows how a spammer can use a dialup PC 1080 running a SMTP direct program 1081 that is able to establish SMTP connections 1044 directly to the SMTP port of the target mailhost. The term "dialup" as used herein refers to a class of Internet subscribers characterized by an inability to service incoming mail requests (i.e., not a mail server), having a related if not sequential name space, often using dynamically-assigned addresses, and generally existing at the lowest tier of pricing offered by an ISP. It includes various means of connecting, not all of which involve literally dialing in to the ISP, for example, wired cable or pocket radio. The spammer typically provides a single copy of a message 1082 and a list of addresses 1083. The program establishes an SMTP connection 1044 to each remote MTA 1045, delivers the message, and proceeds to the next entry in the address list.

Brief Summary Text (49):
Because the Dialup SMTP Direct program 1081 runs under the control of the spammer, the program can be configured to forge any email address, hostname, or any field (e.g., the From: address) in the message header. Consequently, a message received by a user 1048 that is sent by this means may appear to be sent by a co-worker, from one's manager, from friends on another network, or even by the recipient himself

Brief Summary Text (52):
The solutions that are presently available to block junk mail fall into seven general categories. First, the use of centralized blacklisting databases, such as described above for the RBL, IMRSS, and DUL. Second, the use of local blacklisting databases, such as sendmail checking a local database and blocking email that matches entries in the database. Third, blocking mail from nonexistent domains, such as for instance if sendmail receives "MAIL From: <sender@nonexistent.dom>", it will reject the mail because it cannot find the domain "nonexistent.dom" listed in the Domain Name System (DNS).

Brief Summary Text (53):
Fourth, whitelisting methods are used, so that a filter can reject all sender addresses that are not included in a local whitelist of permissible addresses. Fifth, Bcc filtering may be used to reject email from unknown hosts that do not list the recipient's email address in the header of the message. And sixth, client methods may be used to reject junk mail located in the user's mailbox without downloading the mail to the user's mail program (UA). Filtering of client protocols such as POP provides relief to individual users, but still allows junk mail to be stored on the SMTP server.

Brief Summary Text (54):
Seventh, secure electronic mail, such as based on the emerging Secure/Multipurpose Internet Mail Extension (S/MIME) and OpenPGP standards uses public key cryptography to provide security services such as secrecy (confidentiality), integrity (ability to detect modification), authentication, and non-repudiation. Spammers are unlikely to use integrity and non-repudiation services, in particular, since these involve a digital signature signed with the sender's private key. However, these systems do not provide a solution to spam, since not everyone uses public key cryptography. Further, these services typically operate as part of the User Agent, so S/MIME or OpenPGP-protected spam can still be relayed or sent from dialup computers.

Brief Summary Text (56):
It is therefore a primary object of the invention to provide an email filtering system and method. It is another object of the invention to provide an email filtering system that substantially eliminates security risks and loss of company resources associated

with junk mail. It is another object to provide an email filter that operates at the MTA level and performs active filtering based upon characteristics of the incoming connection and the remote host.

Brief Summary Text (57):
In accordance with these objectives, an Active Filter proxy in accordance with a preferred embodiment is provided in a conventional firewall configuration between a remote host and a local MTA. The Active Filter proxy probes the sending host at the time it connects and implements a series of tests to determine if the remote host is likely to be either a dialup customer (Active Dialup testing), or an open relay (Active Relay testing). It also queries the mail server that handles email to the supposed sender of the message to determine if the mail server will accept email for that address (Active User testing). Together, these tests address the primary sources of junk mail.

Brief Summary Text (58):
These tests reject SMTP email based on characteristics of the received SMTP protocol fields and the configuration of the remote host. The Active Dialup test considers certain characteristics typical of dialup PCs, which include the inability to operate as a server and generally a sequential naming scheme. The Active Relay test concludes that if the remote host appears to relay for a test connection, then it will probably relay for spammers. The Active User test detects obvious forgeries by blocking email where the configured mailhost for the sender will not accept a reply to that address.

Brief Summary Text (61):
Minimal involvement is required by email administrators, when compared with the administrative cost of removing junk mail from mail servers, cleaning up after a virus or other malicious code attack, complaining about junk mail, and solving other problems. Administrator involvement generally consists of reviewing logs and adding IP address blocks and domain names to trusted databases where necessary.

Brief Summary Text (62):
It is not practical, and perhaps not possible, to blacklist all current and future sources of spam, or to whitelist all benign sources of legitimate email, because the Internet grows and changes so quickly. However, it is readily possible for most administrators to define the relatively few (perhaps tens or hundreds) trusted domain names and to rely on the Active Filtering methods to characterize the remainder of the hosts that connect.

Brief Summary Text (64):
The present invention is compatible with all known SMTP MTAs. The architecture permits a natural separation of responsibilities for the proxy and the MTA. The proxy offloads the rejection of junk mail, so that the MTA need only consider legitimate email. The MTA may provide other conventional spam-filtering methods of its own (for example, rejecting non-existent MAIL From domains) or may reject mail because the RCPT user does not exist on the local network.

Drawing Description Text (2):
FIG. 1 depicts a prior art illustration of the general architecture for Internet electronic mail using the Simple Mail Transfer Protocol (SMTP).

Drawing Description Text (3):
FIG. 2 is a prior art illustration of a graphical representation of an exchange of SMTP protocol messages involved in transferring a single electronic mail message from one MTA to another.

Drawing Description Text (5):
FIG. 4 is a prior art illustration that shows how a bulk mail program takes advantage of an open relay host elsewhere on the Internet to store a single message and a list of addresses, causing the relay to forward the message to each address in the address list at recipient MTAs. Spammers typically use relaying to offload processing from their computer and obscure their involvement in sending the message.

Drawing Description Text (7):
FIG. 6 is a prior art illustration that shows how spammers may transfer mail directly from a SMTP direct program on a personal computer to the input port of a MTA. Spammers typically use this method to make message forgery easier and to avoid their network's controls on outgoing email.

Drawing Description Text (9):
FIGS. 8-12 show specific architectures in accordance with the present invention when deployed with other email processing systems.

Drawing Description Text (13):
FIG. 12 shows how a proxy may be chained with a content-filtering proxy for enhanced control over incoming email.

Drawing Description Text (14):
FIG. 13 shows an overview of the protocol transactions exchanged in transferring a single email message from a remote host, the Active Filtering proxy server, and the protected MTA.

Drawing Description Text (15):
FIGS. 14-23 show the details of the protocol interactions and processing flow for the transfer of a single email message from a remote host 1400, through an Active Filtering proxy server 1401, to a local MTA 1402.

Drawing Description Text (23):
FIG. 21 shows the transfer of the data in the email message (header, body, attachments, etc.) and how the connection is closed.

Detailed Description Text (7):
Configuration databases include Trusted DB 1093, which is used to identify trusted networks that are permitted to bypass further filtering; Whitelist DB 1094, which contains individual email addresses that are permitted to bypass further filtering; Blacklist DB 1095, which identifies IP addresses of remote hosts that will be blocked immediately after they connect to the proxy server; Relay DB 1096, which contains configuration data for the Active Dialup filter, including addresses of untrusted hosts that are known not to be dialup clients; Dialup DB 1097, which identifies untrusted hosts that are known not to be dialup clients; Configuration DB 1098, which includes general data such as the IP address and port for the Mailhost 1105, permissible domain names for RCPT messages, etc; and System Log 1099, as typically provided by the UNIX syslog facility or Windows NT Event Log service. The preferred embodiment is for each database to be provided as a separate file. However, alternative embodiments may provide for merging some or all databases into a single configuration database, however preferably excluding the Log 1099.

Detailed Description Text (21):
As shown in FIG. 12, the Active Filtering proxy 1104 (on firewall host 1103) can be chained with other proxy servers 1116 (on firewall hosts 1114) to perform other mail filtering functions. For example, various products, such as in accordance with U.S. Pat. No. 5,623,600, provide filtering of viruses and other malicious code. Preferably however, the Active Filtering proxy 1104 is the first host in the chain of proxies, that is, closest to the Internet, so it is best able to determine the essential characteristics of the remote host that is attempting to send email. The two filtering proxies 1104 and 1116 provide improved filtering by requiring each message to pass through both filters before it can be accessed at a client workstation.

Detailed Description Text (23):
With respect to FIGS. 8-12, there does not necessarily have to be a one-to-one relationship between the number of Active Filters and the number of MTAs within an organization. For example, in FIG. 8 based upon performance and loading considerations, there might be three firewall hosts 1103, each connected to the LAN 1102, each running an Active Filtering Proxy process 1104, each having its own unique IP address, and each being configured as a MX host within the organization's DNS database. All three proxy servers 1103 would connect to the MTA 1106 only when they have legitimate (non-dialup, non-relayed, non-forged) email to deliver. While the individual active filtering processes themselves involve additional time and computing resources, these offload the processing of junk mail in such a way as to reduce the overall load on the MTA 1105.

Detailed Description Text (26):
FIG. 13 provides an overview of the present invention, with more detailed operation shown in FIGS. 14-23. The figure shows the key steps used by the Active Filter Proxy 1401 to validate a single email message from a remote host 1400 and transfer the message to the protected MTA 1402. A separate SMTP connection 1418 is used for actively probing the remote host in order to perform Active Dialup 1420 detection and Active Relay 1450 detection. An additional connection may be established to a different mailhost for Active User testing. The Active Filter Proxy 1401 corresponds to proxy

1104 shown in FIG. 7.

Detailed Description Text (27):
The proxy 1401 is shown in FIG. 13 connected between the remote host 1400 and the local MTA 1402. The proxy 1401 and MTA 1402 may be located at separate hosts, as shown in FIGS. 8 and 12, or at a same host as shown in FIGS. 9-11. Because the proxy 1401 controls when it reads data on the connection 1403, it is not possible for the remote host 1400 to proceed with transfer of its message until the proxy 1401 completes its filtering. The proxy only handles incoming email and does not process outgoing email from the MTA to remote hosts. Outgoing email is sent directly from the MTA 1402 to the network.

Detailed Description Text (28):
With respect to Internet standards, the present invention may be implemented without any changes to SMTP or any other protocol. Rather, this method uses multiple SMTP connections, appropriately timed to permit the proxy server to characterize the remote host 1400. Thus, the SMTP connection 1403 is initiated by the remote host 1400, and involves transactions 1410, 1413, 1480, 1484, 1488, 1493, and 1495. The SMTP connection 1418 is initiated by the Active Filtering proxy 1401, and involves transactions beginning at step 1450. This session is used only to acquire protocol responses from the remote host 1400. It does not actually send an email message from the proxy server 1401 to the remote host 1400. In addition, the proxy server 1401 makes other connections to DNS name servers and, if the connection 1418 fails, may make an SMTP connection to the Mail Exchange (MX) host for the address given in step 1413.

Detailed Description Text (29):
Taken together, the processing performed by the Active Filtering proxy 1401 involves the following actions when a remote host 1400 establishes a TCP connection 1403 to the proxy. First, as shown at step 1406, the proxy server 1401 gets the IP address of the remote host and compares the IP address with a database of disallowed addresses. If the IP address of the remote host 1400 matches an entry in the database, the proxy server closes the TCP connection 1403 without transferring an email message. This is described in greater detail in FIG. 14.

Detailed Description Text (30):
At steps 1410 and 1413, the proxy server processes the HELO (optional) and MAIL messages from the remote host 1400. The MAIL message contains the address of the purported sender of the incoming message, which is commonly forged in junk email. Except for trusted addresses (e.g. trusted hosts or whitelisted addresses) and other reverse test connections 1418 (to prevent cycles of reverse test connections), the proxy attempts to open a reverse test connection 1418 to the remote server host. The response (or lack of response) from the remote host dictates the subsequent processing flow.

Detailed Description Text (31):
If the proxy cannot open the reverse connection, it may be because the remote host is a dialup workstation. Accordingly, the proxy then performs Active Dialup testing 1420. Internet service providers typically block service requests (such as SMTP) to their dialup customers using dynamic IP addresses (e.g., assigned by Dynamic Host Configuration Protocol, DHCP, which automatically assigns IP addresses to client stations logging onto a TCP/IP network). The proxy then uses certain heuristics based on the name of the host and its neighbors to categorize the host as a dialup or non-dialup. If it categorizes the host as a dialup, the proxy closes connections 1403 without transferring the email message. Otherwise, it performs Active User testing of the Mail Exchange (MX) host for the From address given in the MAIL message. Active Dialup is described more fully with respect to FIGS. 16-17.

Detailed Description Text (47):
At step 1408, if the remote host is blacklisted, the proxy 1401 issues an error reply to the remote host (e.g., "550 SMTP administratively blocked"), closes the connection 1403, logs the rejected connection, and exits without any email being transferred. The system log 1099 (FIG. 7) may be configured to log on the local host or on a remote host, such as the local MTA 1402. If the remote host 1400 is trusted or the IP address acquired in 1404 does not match any entry in the blacklist 1406, then the Active Filter displays the SMTP greeting message, step 1409.

Detailed Description Text (53):
At step 1413, the remote host 1400 sends a mandatory MAIL From message to the proxy 1401. At step 1414, the proxy reads the message from the TCP connection. The message

must contain an email address, represented as "<mfaddr>", in the Internet address format consisting of the concatenation of a user name, "@" sign, and domain name. The term "MAIL From address" refers to the entire address passed in the MAIL From message, and the term "MAIL From domain" refers to the domain name to the right of the "@" sign.

Detailed Description Text (54):
At step 1415, the proxy checks the MAIL From address to determine if the remote connection is from another Active Filtering proxy 1401. For instance, suppose host A and host B both have an Active Filtering proxy handling incoming email connections. Host A opens a data connection to host B. In turn, host B opens a reverse test connection back to host A. When this happens, host A must recognize the reverse test connection so that it does not propagate a cycle where each proxy opens reverse test connections to the other, until either the initial connection is terminated or one of the proxies runs out of resources.

Detailed Description Text (56):
In accordance with the preferred embodiment of the invention, the Active Filtering proxy uses the reserved address "reverse" with the local domain name on each reverse test connection. This reserved address is used by all Active Filtering proxies. Continuing with step 1415,. the proxy 1401 checks the MAIL From address to determine if it contains the reserved name "reverse" before the @ symbol. If so, the proxy issues an error reply 1416 on the incoming connection and exits. The receiving proxy then closes the connection when it detects this address to prevent abuse by spammers who might learn this reserved address. In this case, the remote host (e.g., the proxy at host B) will not be able to test the local host (e.g., host A), but email will still be possible.

Detailed Description Text (58):
In the preferred embodiment, the whitelist file is a text file that contains addresses (one per line) that are periodically mined from sendmail log entries for outgoing ("to=") messages. These log entries are for mail sent by the local organization to destination addresses on other networks, so adding these destination addresses to the whitelist file will ensure that the proxy will permit incoming email from those persons that local users have sent mail to. However, the whitelist database may be implemented as a hashed database (e.g., dbm) files, or even could be disabled. If the address matches a whitelist entry, processing continues with step 1470. The difference between the trusted database 1093 and the whitelist database 1094 is that for trusted hosts, mail is permitted from any user on the remote host to any user on the local host. For whitelist entries, mail is permitted only from the named user on the remote host to any user on the local host.

Detailed Description Text (63):
As noted above, email from dialup PCs running direct SMTP programs is a major problem since the spammer can use the program to forge any protocol field or message header field. Approximately one-third of the junk mail attempts are from ISP dialup addresses. The spammer almost always uses a relatively inexpensive "throwaway" dialup account with an Internet service provider (ISP). These dialup accounts typically have certain characteristics imposed by their respective ISPs. Because of the use of dynamic name allocation (e.g., DHCP) and because of pricing strategies, the ISP permits the user to only operate as a client. That is, the ISP uses its packet routers to block network service requests such as SMTP to their dialup users. The second characteristic of dialup accounts is that most ISPs use a regular naming scheme for such dialup addresses so as to simplify maintenance of the DNS database. The names frequently include decimal or hexadecimal representations of the last byte of the IP address.

Detailed Description Text (76):
At step 1425, the proxy 1401 issues an SMTP error message (e.g., "550 apparent dialup") and exits, thus closing the data connection without any email being transferred. In the preferred embodiment, the proxy also logs the rejected dialup and adds the IP address of the remote host to the blacklist database.

Detailed Description Text (98):
The proxy 1401 performs Active Relay Testing by testing the validity of the MAIL From address on the reverse connection and implementing a relay test, such as the one shown in FIG. 5. These tests are conducted while the remote host 1400 is connected to the proxy 1401 as a factor in determining whether to accept the remote host's message. If the remote host 1400 gives an indication that it will not accept a reply email message to the purported sender or that it will relay a test message from the proxy 1401, then

that remote host is at an increased risk for relaying mail from someone else to the local MTA 1402. On the other hand, if the remote host indicates that it will accept a reply message for the sender and that it will not relay for the proxy, then the remote host probably is not an open relay.

Detailed Description Text (99):
The proxy 1401 performs this test using the reverse SMTP connection 1418, then continues with the protocol transactions in steps 1454, 1456, 1458 and 1465. The test simply monitors the responses from the remote host, and does not actually send an email message to the remote host 1400. The local MTA 1402 is not involved in this test.

Detailed Description Text (106):
In steps 1458 and 1460 the proxy determines if the remote host will accept the address of the supposed sender of the message. This may appear to be designed to determine the actual existence of the user "mfaddr" as is performed by the Active User test at step 1901 and there is some overlap if "mfaddr" actually exists at the remote host 1401. However, in the general case, this step is designed to determine if the remote host is configured to deliver (either locally or by relaying) email to the supposed sender. If at step 1460 the reply is "250" then the remote host will accept mail to this address, so the proxy continues with step 1462. Otherwise, if the reply is anything other than "250", the proxy sends an error response 1461 on the data connection 1403 and exits, thus closing the data connection 1403 and the reverse connection 1418. In the preferred embodiment, the proxy also writes a system log entry for the rejected message and adds the remote host's IP address to the blacklist database 1095 (FIG. 7) before exiting.

Detailed Description Text (108):
At step 1462, the proxy 1401 attempts to find if the IP address of the remote host 1400 matches a non-relay entry in the Relay database 1096 (FIG. 7). This database lists blocks of addresses that the local organization must exchange email with, but which would fail the relay test. There might typically be between about 5-50 entries in this database, with each entry covering a block of addresses. These entries can be pre-defined by a site survey performed by each organization, preferably before installing the Active Filtering proxy server. For simplicity, the preferred embodiment of the Relay Database 1096 (as with other IP addresses listed in steps 1406 and 1413) expresses these addresses as a dotted-quad IP address, a forward slash "/", and a number of bits to be matched. Other embodiments may use other representations (hashed lists, dbm filed, or CAM) for performance reasons.

Detailed Description Text (115):
If the proxy responds with a "250" to both RCPT messages, then it is not possible to tell if the MAIL From address 1413 is legitimate or not. In the previous example, a legitimate message from <someone@smallhost.dom> may be sent via an open relay smarthost smtp.bigisp.dom. Alternately, the message could well be forged, since the remote host is an open relay. For example, referring to step 1064 of FIG. 4, the spammer forged the MAIL From address "good@relay.dom". Thus, when the proxy receives "250" responses to both messages, the preferred embodiment of the Active Relay method is to reject the message and log its rejection. If a subsequent review of rejected messages shows a legitimate address, the administrator of an Active Filtering proxy can then add the individual address to the whitelist database (FIG. 7, item 1094) or can bypass relay testing for smtp.bigisp.dom by defining it as a non-relay in the Relay database 1096 (FIG. 7).

Detailed Description Text (116):
The remote host may also respond with a "550" (for example) to message 1458 and a "250" to message 1465. Some hosts will permit promiscuous relaying but reject any non-existent local addresses. In this case the proxy rejects the email message.

Detailed Description Text (118):
The administrator may manually edit the relay database to add an IP address if a review of log entries shows that the remote host is an authorized "smart host", i.e., a host authorized to handle the local network's outgoing email. In addition, certain MTA programs give a "250" reply to the RCPT message 1465, but then discard the message later on. These may be configured as trusted or as non-relay.

Detailed Description Text (119):
The active relay method permits automatic rejection of all email sent from a user at an open relay host or relayed by an open relay host. However, in some cases it is necessary to override this behavior, for business or other reasons. For example, with respect to the bigisp example given above, the administrator of the Active Filtering

proxy can configure the proxy to permit email sent from smallhost.dom and relayed by bigisp.dom by any one of the following actions: (1) defining bigisp.dom as a trusted domain, (2) defining smallhost.dom as a trusted domain, (3) adding a whitelist entry for the specific address "user@smallhost.dom", (4) or adding a non-relay entry for bigisp.dom, even though it is an open relay.

Detailed Description Text (124):
The Active User method illustrated in FIG. 19 determines if the MAIL From address 1413 is acceptable to a mailhost 1900 configured to receive email for the MAIL From domain. By convention, this mailhost is either a Mail Exchange (MX) host or the host identified in the MAIL From message. This method uses the same SMTP messages described for the Active Relay method (FIG. 18, steps 1454-1458), but in most cases the proxy accesses a different mailhost than the remote host 1400. While the Active Relay test is concerned with determining if the remote host 1400 is at risk for sending relayed or forged email, the Active User test accesses the mailhost 1900 responsible for receiving email for the MAIL From domain to determine if it will accept email for that address. If it does not accept the MAIL From address, then this indicates that the MAIL From address is probably forged and does not exist on that network.

Detailed Description Text (125):
For example, assume the remote domain remote.dom has two mail servers, out.remote.dom for sending outgoing email and mx.remote.dom for receiving incoming email. If the proxy 1401 receives a connection 1403 from out.remote.dom, the proxy will be unable to establish a reverse test connection 1418 to that particular host because it is not configured to accept incoming SMTP connections. Assuming that the host names surrounding out.remote.dom do not appear to be dialups, it remains for the Active User method to attempt to validate the MAIL From address. In this case the proxy 1401 would find the MX host mx.remote.dom and query that host as to the validity of the MAIL From address.

Detailed Description Text (130):
It is noted that for some networks where the same host handles both incoming and outgoing email, the mailhost 1900 may be the same (that is, have the same IP address) as the remote host 1400. In this case, the proxy simply makes a second test connection to the same host without regard to having previously tested the MAIL From address at this host.

Detailed Description Text (137):
In step 1470 the proxy connects to the MTA using the same method described for the reverse test connection 1418. In summation, the proxy connects to the MTA for messages with any of the following characteristics: connection from a trusted domain (step 1417); trusted MAIL From domain (step 1417); whitelisted MAIL From address (step 1417); or email from a user with an account at a non-dialup, non-relay host (step 1467). In addition, subject to the validity of the user address as determined in step 1913, the proxy will permit mail from hosts where the reverse connection fails, but host is configured as non-dialup (step 1421); reverse connection fails, but host is not detected as a dialup (step 1424); reverse connection succeeds, but relay test is inconclusive (steps 1454, 1456, 1458); reverse connection succeeds, but host is configured as non-relay (step 1462) or reverse connection succeeds, MAIL From address matches connecting host, and the proxy is configured for loose relay testing (steps 1463, 1464).

Detailed Description Text (143):
FIG. 21 shows the processing steps involved in transferring the actual email message from the remote host 1400 to the MTA 1402. Except for the limited filtering performed in steps 1491 and 1492, the proxy transparently transfers the SMTP DATA command 1484, message header lines 1488, message body lines 1490, 1493, and closing protocol lines 1495 from the remote host 1400 to the MTA 1402. By convention, the message header is defined as all lines of the message down to, but not including, the first empty line. The proxy also transparently transfers SMTP replies from the MTA to the remote host (steps 1486 and 1497). As is consistent with SMTP, the lines of the message header and message body are not individually acknowledged by the MTA.

Detailed Description Text (147):
This ends the transfer of the single SMTP email message associated with the current instance of the proxy 1401, and the proxy 1401 exits. In the preferred embodiment, multiple messages from multiple remote hosts are handled by relying on the proxy server's operating system 1090 (FIG. 7) to run multiple instances of the proxy process, one for each message. However, other implementations are consistent with this invention

such as, for example, a multi-threaded proxy server process that handles multiple messages.

Detailed Description Text (150):
In addition, in the event that it becomes illegal to connect to any mail server except to transfer legitimate email, a message may be transferred to the MAIL From address saying "We have received your SMTP connection and are considering whether to accept your email message." The preferred embodiment tests for relaying only for non-trusted hosts who attempt to deliver mail to the local MTA.

Detailed Description Text (151):
While the preferred embodiment uses Internet standard protocols such as IPv4, DNS, TCP, and SMTP, the invention may also be used with other networking protocols and network architectures, such as, for instance, IP version 6 (IPv6) or X.500 name services, or protocols not yet developed. Further, the invention may be used with other backbone MTA-to-MTA protocols such as Extended SMTP (ESMTP), the X-400 Message Handling System (MHS) or client-to-mailhost protocols such as POP or IMAP when the Active Filtering functions are not performed on the backbone. Further yet, the invention may be used with various cryptographic architectures such as Secure Socket Layer (SSL), IP Security (IPSec), S/MIME or OpenPGP standards, although spammers are unlikely to use any protocols involving traceable encryption keys.

Other Reference Publication (4):
Cauce, Coalition Against Unsolicited Commercial Email, www.cauce.org, 2 pages.

Other Reference Publication (6):
Spam-Free Email Account Services, www.mailcircuit.com/hand.htm, 1 page.

CLAIMS:

14. The system of claim 1, further comprising an electronic mail address filter having a whitelist database, wherein said system establishes a connection to the remote host if a mail from address of the sender is in the whitelist database.

25. The system of claim 1, wherein the electronic message comprises an email.

WEST

Generate Collection Print

L4: Entry 6 of 8 File: USPT May 8, 2001

DOCUMENT-IDENTIFIER: US 6230188 B1
** See image for Certificate of Correction **
TITLE: System and method for providing a proxy identifier in an on-line directory

Abstract Text (1):
A method for protecting the privacy of a person's email address that is maintained in an on-line directory service (14). The directory service includes a database (16) having actual email addresses and a processing system (20) that is available for retrieving these listings from the database. The method includes the computer implemented steps of receiving from a user a request for a person's email address; determining whether or not a record is present in the database that corresponds with the user request; and if a record is present that includes a person's actual email address, then automatically displaying a selectable proxy email address (38) in lieu of the person's actual email address. The proxy email address is provided without having been requested by the person and without requiring the processing system to determine whether or not the person prefers to have a proxy email address displayed or the person's actual email address displayed. The proxy email address includes a selectable portion that enables the user to send an email message to the person without knowing that person's actual email address.

Brief Summary Text (2):
The present invention relates to on-line directory services, and more particularly to on-line directory services for obtaining email addresses.

Brief Summary Text (7):
The '769 registration system for altering the display of an e-mail address and providing a knock--knock feature is useful, however, it has a number of disadvantages. A first disadvantage is that unless a user is aware of that particular on-line directory service, then the responsibility of determining whether a user would like to keep his or her listing information private is up to the on-line directory service. It is cumbersome, as well as unlikely, for an on-line directory service to take the time necessary to poll each individual listing as to whether he or she would prefer to have their information public or private. Thus, it is highly likely for an on-line directory service to unwittingly make public, email address information that a person would prefer to have kept private.

Brief Summary Text (8):
A second disadvantage is that the '769 patent is that it is cumbersome. It appears to require the person to register with the on-line directory service and to select a privacy option before being able to allow the third party listing to take advantage of such a feature. Most people are unwilling to go to the effort of registering in order to take advantage of such a system, especially since the person may not even know that their email address is listed with that particular directory service and further may feel that since the listing is shown publicly to begin with, there would be no point in now making it private.

Brief Summary Text (9):
A third problem is that spammers routinely gather e-mail information from on-line directory services and resell this information to individuals and businesses for marketing purposes. These e-mail addresses are sold in large batches and contain e-mail addresses from all over the world. While spam e-mail is undesirable in the United States simply because it wastes computing resources and is a nuisance to clear out of one's e-mail box, it is a much more significant problem in Europe where many countries charge their e-mail addressees for each piece of e-mail received.

Brief Summary Text (12):

In accordance with aspects of the present invention, a method for protecting the privacy of a person's full email address in an on-line directory service database record is provided. The directory service includes a processor available for retrieving such listings from the database. The method includes the computer implemented steps of receiving from a user a request for a person's email address and determining whether or not a record is present in the database that corresponds with the user request. If a record is present that includes a person's actual email address, then the processing system automatically displays a selectable proxy address in lieu of the person's actual email address. The proxy address is provided without having been requested by the person and without requiring the processing system to determine whether or not the person prefers to have a proxy email address displayed or the person's actual email address displayed. The proxy email address includes a selectable portion that enables the user to send an email message to the person without knowing that person's actual email address.

Brief Summary Text (13):
In accordance with other aspects of this invention, an on-line directory service is provided including a database of information including actual email addresses and a processing system. The processing system receives a user request for an actual email address and in response, determines the actual email address from the database. Upon finding the actual email address, the processing automatically provides the user with a selectable proxy email address and not the actual email address.

Drawing Description Text (5):
FIGS. 3 and 4 are flow charts illustrating a method of processing a user's request for an email address formed in accordance with the present invention.

Detailed Description Text (4):
Still referring to FIG. 1, the directory service 14 includes an email server 18 and a processing system 20. The processing system 20 has a number of computers, or gaters, each of which is linked to the storage either directly or through an intermediate switching network. A user accesses the directory service over the Internet and through a firewall that protects the service from external tampering.

Detailed Description Text (5):
Referring to FIG. 2, when the user accesses the service through a standard URL identifier, the processing system 20 provides to the user a menu 22 that includes one or more request choices for finding various types of data available from that particular directory service. These choices are selected using a keyboard or pointing device, such as a mouse or trackball. Shown in FIG. 2 are the choices to "FIND PEOPLE", "FIND ADDRESS", "FIND EMAIL", etc. Upon selection of the FIND EMAIL choice, the user is provided with another display page 24 requesting the user to enter various search parameters.

Detailed Description Text (6):
In FIG. 3, when the user selects the menu item to find email an address, the processing system 20 receives the request at block 26 and in response provides at block 28 an entry screen with fields for the user to enter various types of data useful in searching for the correct listing. This may include such items as a name or address. The user enters this information and submits the parameters to the processing system using selection buttons on the web page. The system receives the entry parameters at block 30 and conducts a search of the database to find the record (or records) that match the entry parameters at block 32. If no match is found, a display message is provided back to the user at block 34.

Detailed Description Text (7):
If one or more matches are found, the logic proceeds to FIG. 4, where the processing system 20 prepares a proxy email address 38 for each record found at block 40. The processing system 20 displays each search result at block 42 using the prepared proxy email address 38 instead of the record's actual email address. In one embodiment, the proxy email address 38 includes a first portion and a second portion. The first portion is provided in lieu of the listing's alias, or user name, and is given as a selectable word, such as "Send", with underlining to indicate to the user that the text is a selectable link. The second portion is given as the listing's domain name. This is helpful to users in order to narrow the selection of a party of interest when more than one person is matched for a given set of entry parameters. Other formats of proxy email addresses may be used.

Detailed Description Text (8):

In a second embodiment, the proxy email address 38 includes two selectable portions. A first selectable portion is similar to the first portion described in the embodiment above. A second selectable portion is provided that, once selected, allows the user to send an email message to all persons in that domain. Alternatively, a second selectable portion may be provided that, once selected, gives a list of all users on that domain as known in the directory service. In another alternative embodiment, a second selectable portion is provided that, once selected, provides information to the user regarding that particular domain service. As will be appreciated, other embodiments of selectable and non-selectable portions are possible.

Detailed Description Text (9):
Still referring to FIG. 4, the processing system 20 checks at block 44 to determine whether the user has selected the proxy email address. If so, the processing system 20 provides the user at block 46 with an email entry screen having one or more entry boxes for the user enter information relevant to the email message. For example, in one embodiment, the user may enter a subject description, the user's name, and a message for the receiving party. Also included is a box for entering the user's email address. This address is required for embodiments in which the user wishes the recipient to respond back directly to the user. This address is optional for embodiments in which the user wishes to remain completely anonymous.

Detailed Description Text (10):
Once the user has entered the data in the email entry page, the user selects an item on the display screen that causes the data to send the information to the processing system where it is received at block 48. The processing system 20 creates an email message using this input information at block 50. In one embodiment, the created email message shows the directory service as the sending party and indicates in the email message text the user's inputted email address as the true sender. In another embodiment, the created email message shows the user's inputted email address as the sender. In yet another embodiment, the created email message shows the directory service as the sending party and does not include any mention of the user's email address of the user as the true sender. If the user did not provide a return email address, the directory service furnishes the user with a identification means that allows the user to pickup return email messages from the directory service. For example, the user is provided with a randomly-generated reference number. The user may request via telephone, email, or web access, any messages corresponding to that reference number.

Detailed Description Text (11):
Numerous variations in the types of messages actually sent to the listing party are possible. In one embodiment, the directory service provides a marketing banner or tag at the end of the email message text, indicating that the service was sponsored by a particular business, for example. In another embodiment, a message is inserted explaining to the recipient that the user does not have the person's actual email address, but instead is using the directory service to contact the person in a privacy-respecting manner. In another embodiment, a message is inserted warning the recipient that by hitting the reply button in response to this message, will cause the person's actual email address to be sent to the user-sender. Once the email message is prepared, the processing system 20 sends the email to the listing party at block 52. A display is preferably provided at item 54 to the user indicating the status of the send email, i.e., whether it was accomplished successfully, whether it was put into a queue, or whatever the case may be.

Detailed Description Text (12):
As will be appreciated from a reading of the above, the present invention greatly increases the privacy of an individual with regard to their email address. This is accomplished in an automatic manner, so that even if a listed party is not aware that they are listed with that particular directory service, the listed party is in no jeopardy of having their email address made publicly available through the directory service. In addition, even if the party is aware that they are listed with a particular directory service, the person does not have to go to the trouble of registering with the service and/or altering the status of whether their email address is to be shown.

Detailed Description Text (13):
In accordance with the present invention, a person's actual full email address is preferably not ever provided, even though the person would like to have their email address made public. This helps to reduce the amount of spam email. It is possible to practice the present invention by allowing the person to change his or her email address from being private to being public, though it is not preferred.

Detailed Description Text (14):
The present invention also aids in reducing the damage caused by spam email by reducing public access to email addresses. While the preferred embodiment of the invention has been illustrated and described, it will be appreciated that various changes can be made therein without departing from the spirit and scope of the invention. For example, currently people and/or machines are known to scan web sites for email addresses. Once obtained, these email addresses are collected and sold to spammers. The present invention may be used by web page owners to protect those email addresses listed on their web site pages, thereby prohibiting the collection and subsequent sale of their email address and consequently reducing junk email. Thus, it is to be appreciated that the present invention email proxy system could be applied to any web page containing an email address in which the recipient prefers to have an email address that is private while still retaining the ability to receive emails.

CLAIMS:

1. A method for retrieving listings from a database, the method comprising:

(a) obtaining a request for a party's email address;

(b) determining whether a record is present in the database that corresponds with the request; and

(c) if a record is present that corresponds to the request, then automatically displaying a selectable proxy address in lieu of the party's actual email address; the proxy address being displayed without requiring participation by the party and without determining whether the party prefers to have a proxy email address displayed;

wherein the proxy email address includes a selectable portion that enables a sender to send an email message to the party without knowing the party's actual email address.

2. The method according to claim 1, wherein the proxy email address includes a selectable first portion and a second portion, the second portion including a reference to a domain name associated with the party's email account.

3. A method for providing a proxy identifier in an on-line directory, the method comprising:

obtaining a request for an email address, wherein the request includes one or more attributes for identifying the email address;

obtaining at least one record associated with the one or more attributes from a listing database; and

automatically displaying a selectable proxy address corresponding to the at least one record;

wherein the selectable proxy address enables a sender to send an email communication without knowing an actual email address; and

wherein the automatic display of the selectable proxy address is performed without participation by a party associated with the email address and without determining a privacy setting for any matching records.

4. The method as recited in claim 3, wherein the proxy address includes a selectable first portion and a second portion, the second portion including a reference to a domain name associated with the party's email account.

5. The method as recited in claim 3 further comprising:

obtaining a selection of the selectable proxy address; and

displaying a data entry display to enable the user to prepare a message, wherein the data entry display allows the sender to prepare a message to the party corresponding to the email address.

6. The method according to claim 1, wherein the email message includes an additional message regarding the context under which the message is being sent.

7. The method according to claim 1, wherein the email message includes a marketing message.

8. The method according to claim 1, wherein the email message does not reveal the identity of the sender.

9. The method according to claim 1, wherein the email message identifies an actual email address of the sender.

10. The method according to claim 9, wherein the email message includes a warning message indicating that replying to the email message will cause the person's email address to be divulged to the sender.

11. An on-line directory service comprising:

(a) a database of information including actual email addresses;

(b) a processing system that receives a user request for a party's actual email address and in response, determines the actual email address from the database; upon finding the actual email address, the processing automatically provides the user with a selectable proxy email address and not the actual email address;

the proxy address being provided without having been requested by the party and without requiring the processing system to determine whether the party prefers to have a proxy email address displayed;

wherein selection of the proxy email address enables the user to send an email message to the party without knowing the party's actual email address.

12. The on-line directory according to claim 11, wherein the proxy email address includes a selectable first portion and a second portion, the second portion including a reference to a domain name associated with the party's email account.

13. The on-line directory service according to claim 11, wherein upon selection of the selectable portion of the proxy email address, the processing system provides a data entry display that enables the user to prepare a message to the party.

14. The on-line directory service according to claim 13, wherein after entering the information on the data entry display, the user transmits the information to the processing system; the processing system then preparing and sending an email message to the person using the information.

15. The on-line directory service according to claim 11, wherein upon selection of the selectable portion of the proxy email address, the processing system provides a data entry display that requires the user to enter their return email address.

16. The on-line directory service according to claim 11, wherein the email message sent to the person includes an additional message regarding the context under which the message is being sent.

17. The on-line directory service according to claim 11, wherein the email message sent to the person includes a marketing message.

18. The on-line directory according to claim 11, wherein the email message does not reveal the identity of the sender.

19. The on-line directory according to claim 11, wherein the email sent to the party identifies an actual email address of the user.

20. The on-line directory service according to claim 19, wherein the email message sent to the person includes a warning message indicating that by replying to the email message using the user's email return address will cause to the person's email address to be divulged to the user.

21. The method as recited in claim 1 further comprising:

obtaining a selection of the selectable proxy address; and

displaying a data entry display to enable the user to prepare a message, wherein the data entry display allows the sender to prepare a message to the party corresponding to the email address.

22. The method according to claim 21 further comprising requiring the sender to enter a return email address.

23. The method as recited in claim 21 further comprising:

obtaining the sender message prepared on the data entry display; and

transmitting an email to the party corresponding to the email address including the sender message.

25. The method as recited in claim 8, wherein the email message identifies the sender by a numeric identifier.

26. The method as recited in claim 25 further comprising:

obtaining a request from a sender to view any email responses to the sender identified by a numeric identifier; and

displaying a set of responses corresponding to the unique numeric identifier of the sender.

29. The method according to claim 5 further comprising requiring the sender to enter a return email address.

30. The method as recited in claim 5 further comprising:

obtaining the user message prepared on the data entry display; and

transmitting an email to the party corresponding to the email address including the sender message.

32. The method as recited in claim 3, wherein the email message includes an additional message regarding the context under which the message is being sent.

33. The method as recited in claim 3, wherein the email message includes a marketing message.

34. The method as recited in claim 3, wherein the email message does not reveal the identity of the sender.

35. The method as recited in claim 34, wherein the email message identifies the sender by a numeric identifier.

36. The method as recited in claim 35 further comprising:

obtaining a request from a sender to view any email responses to the sender identified by a numeric identifier; and

displaying a set of responses corresponding to the unique numeric identifier of the sender.

37. The method as recited in claim 3, wherein the email message identifies an actual email address of the sender.

38. The method as recited in claim 37, wherein the email message includes a warning message indicating that replying to the email message will cause the person's email address to be divulged to the user.

WEST

Generate Collection Print

L4: Entry 2 of 8 File: USPT Dec 17, 2002

DOCUMENT-IDENTIFIER: US 6496855 B1
TITLE: Web site registration proxy system

Brief Summary Text (4):
Before using many websites, internet users need to fill in an often cumbersome registration form providing personal data. Site owners require this information for marketing purposes and to personalise the offering to customers. Registration demands can range from the basic requirement of a name and email address to a detailed request for personal information including street address, employment details and even salary levels. This process gives rise to a number of problems for users. Registration is often slow and not intuitive, with an additional problem that formats differ from site to site. Once registered with more than one site, users also have the problem of keeping track of the different user names and passwords that they use. When a user's information changes (email, addresses etc.) the management of multiple registrations becomes unwieldy. Furthermore, users have little or no control of information released to sites which can on-sell the personal data leading to both a breach of individual privacy and, perhaps inevitably, an accompanying barrage of unwanted direct marketing emails or "spam".

Brief Summary Text (24):
Preferably, the method includes the step of providing a unique proxy address for the user in a registration application so that communications addressed to the user using the unique address are received by the at least one registration agent computer or registration agent server and are subsequently forwarded to the user. More preferably, the communications are forwarded to the user in dependence on an email filtering policy accepted by the user. Most preferably, a different proxy address for the user is allocated for each subsequent registration with other service computers or server nodes.

Brief Summary Text (33):
In terms of the internet user, the benefits of using the interface provided by the registration agent site can be summarised as follows: the interface provides a convenient way of navigating between sites since it is necessary to remember only one password; the interface provides an effortless way of registering with new sites; it offers the ability to effect a global change across sites; it provides for the control of privacy by allowing the user to define a privacy policy; and, it allows for the integration of email filtering by proxy to prevent "spamming".

Brief Summary Text (35):
Referring to FIG. 2, in summary, the service that the interface of the registration agent site 10 provides is one of assisting internet users to complete registration forms for websites by proxy, and logging into their sites on repeat visits. The user does not have to retype information, can have different profiles, can automatically check privacy policies, can review what data has been given out and to whom, and can protect their email address. Indeed, a key component of helping users control their interaction with sites is to protect their email address from being abused by the sites they give it to. The present invention's registration processing system 11 offers the option to give protected email addresses to sites when a user registers through the interface. The site does not receive the user's real address, but is instead given a unique proxy address by the registration processing system 11 (a different one for each site). Email sent to that address is forwarded by the registration processing system 11 to the user's email account. This allows users to selectively cut "spammers" off without having to change their email address. It also allows users to identify which sites are giving their email addresses to third parties which use it for "spam".

Brief Summary Text (36):

In summary, the service that the interface of the registration agent site provides is one of assisting internet users to complete registration forms for websites by proxy, and logging into their sites on repeat visits. The user does not have to retype information, can have different profiles, can automatically check privacy policies, can review what data has been given out and to whom, and can protect their email address. Indeed, a key component of helping users control their interaction with sites is to protect their email address from being abused by the sites they give it to. The present invention offers the option to give protected email addresses to sites when a user registers through the interface. The site does not receive the users real address, but is instead given a unique proxy address (a different one for each site). Email sent to that address is forwarded to the users email account. This allows users to selectively cut "spammers" off without having to change their email address. It also allows users to identify which sites are giving their email addresses to third parties which use it for "spam".

Detailed Description Text (4):
The core service provided by the registration agent site 10 is one of assisting users to fill out forms on websites, primarily targeted towards registering with new sites and logging into sites on repeat visits. The user does not have to retype information, can have different profiles, can automatically check privacy policies, can review what data they gave out and to whom, and can protect their email address. The system does not require any plug-ins or software downloads, and is browser independent.

Detailed Description Text (16):
The registration processing system 11 also allows users the option to give "protected" email addresses to sites rather than their normal address. When a site requests the user's email address, the interface generates a new address in a mail domain and supplies that to the site. Email to the address is forwarded by the registration agent's system to the user's real email address, including a header indicating which site it originated from. Mail is not stored by the system, merely forwarded. The user can disable a protected address to prevent unwanted mail from reaching them.

Detailed Description Text (19):
When registering for the first time with the registration agent site 10, the user is presented with a form generated dynamically to gather the minimum information they need, given the circumstances. Core information required to sign up a new member includes the user's email address (which is subsequently verified). The new member chooses a username and password which is required on all subsequent visits to the registration agent site. If the new member is registering with a new site at this time, the user is presented with a form which sets out the information that the site will want for registration. The user is also presented with the option of filling out data fields required by most affiliated sites which will make signing up with new sites faster next time.

Detailed Description Text (20):
The information may be grouped into different categories, for example: 1. basic information (name, email address); 2. professional contact information (work address and phone number, etc); 3. personal contact information (home address, etc); 4. profession demographics job title, etc); and, 5. personal demographics (size of family, hobbies, interests, dislikes, etc).

Detailed Description Text (23):
In FIGS. 3 and 4, it is assumed that the internet user has navigated the World Wide Web using a web browser (step 100 or 200) to arrive at the login page of a website (referring site), of which they are not already a member, but which is affiliated with the RAS and provides a button or other icon with a URL to the RAS web server. The user is not already a member of the RAS. The user clicks on the RAS button appearing on the login page and a pop-up window appears and the browser window of the referring site goes behind. In step 101 or 201 the user completes the new member section of an entry page, giving a username, password, email address and language. The user then selects an option that says that they are not already a member of the referring site and clicks on an "enter" button. A new page then appears in step 102 or 202 requesting additional information that is necessary for the user to actually register with the referring site. The site requirements are determined by accessing the registration profile database 13. A master user profile for the new member is created and stored in the user profile database 12, together with a personal profile for the new registration. Once the user has provided the additional information, they click "enter" and the user's new home page for the RAS appears (in step 203) showing the referring site as a registered site and a separate list suggesting other affiliated sites where the user may wish to

register. The RAS pop-up window is then hidden behind the referring site window, which itself changes to the page showing that the user has successfully registered with the site.

CLAIMS:

12. A method according to claim 1, in which the communications are forwarded to the user in dependence on an email filtering policy accepted by the user.

WEST

Generate Collection Print

L4: Entry 4 of 8 File: USPT Apr 2, 2002

DOCUMENT-IDENTIFIER: US 6366950 B1
TITLE: System and method for verifying users' identity in a network using e-mail communication

Brief Summary Text (12):
In addition to these security concerns, a further concern is that users can camouflage their real identity, for example, by regularly changing the screen name and/or their return address in an electronic mail message (email).

Brief Summary Text (16):
An aspect of the invention involves a method of maintaining a user identification database that indicates when users are in communication with a network. The method includes the acts of associating in a computer accessible storage medium, electronic mail addresses, processor-embedded identifiers and status information. A first electronic message is received from a first computer. The first electronic message contains an electronic mail address and a copy of the processor-embedded identifier existing in the first computer. The first electronic mail address is used to access the corresponding processor-embedded identifier stored in the storage medium. The processor-embedded identifier from the first computer is compared with the processor-embedded identifiers of the storage medium. The status information in the storage medium is modified to indicate that the first electronic mail address is authentic when the processor-embedded identifier from the first computer matches a processor-embedded identifier of storage medium.

Detailed Description Text (10):
The communications modules, for example, allows communications between the computers 2, 4 in accordance with preferable standardized communications protocols. In one typical application, the communications protocols support the exchange of emails. These communications protocols include a Transmission Control Protocol/Internet Protocol (TCP/IP), a Simple Mail Transfer Protocol (SMTP), a File Transfer protocol (FTP), a Hypertext Transfer Protocol (HTTP) and a Lightweight Directory Access Protocol (LDAP).

Detailed Description Text (11):
The TCP/IP is a protocol that specifies how computers exchange data over the Internet, The TCP/IP handles tasks such as packetization, packet addressing, handshaking and error correction. The SMTP is used to transfer email between computers. Generally, the SMTP is a server-to-server protocol, so other protocols are used to access the messages. The SMTP dialog usually happens in the background under the control of a message transport system. The FTP is a client-server protocol that allows a user on one computer to transfer files to and from another computer over a TCP/IP network. The ITTP is a client-server TCP/IP protocol used on the World-Wide Web for the exchange of HTML documents. The LDAP is a relatively simple protocol for updating and searching directories running over TCP/IP, as described below in greater detail.

Detailed Description Text (13):
Computers can communicate with each other, for example, over the Internet, because each computer can be addressed individually. In such embodiments, certain computers have an assigned Internet protocol address (IP address). The IP address is a 32-bit host address that is usually represented in dotted decimal notation, for example, 128.121.4.5. The decimal IP address is in most cases not known to the user. In addition, most users are not aware that this IP address exists. In addition, in many embodiments, a computer user has an assigned email address that specifies the source or destination of the message. The email address is typically in the form of "name@xyz.com", for example, as known in the art.

Detailed Description Text (14):

In accordance with one embodiment of the present invention, the ID number serves to address, identify and authorize computers. As mentioned above, the ID number is unique to a computer and cannot be altered. This provides a higher degree of reliability and security, because the IP address and the email address can be altered. For instance, some users alter the email address or the address field to camouflage the return address and, thus, their real identity.

Detailed Description Text (15):
Returning to the embodiment illustrated in FIG. 1. The user of the computer 2 writes an email to be sent to the user of the computer 4. When the email is composed and the user initiates transmission to the computer 4 over the communications medium 6, the communications software (e.g., SMTP) automatically converts the email into an appropriate electronic data format. Besides the actual email message, the return email address and the return IP address, the data format includes, in accordance with the present invention, the microprocessor-specific ID number.

Detailed Description Text (16):
The computer 4 receives the electronic representation of the email and converts it back to a user-readable message. During the process of converting, the computer 4 extracts the received ID number and compares (looks-up) it with the ID number(s) stored in the data base 7. When the received ID number matches one of the stored ID numbers, the computer 4 accepts the email as one received from an authorized computer.

Detailed Description Text (17):
The look-up of the ID number is generally triggered by an event. That is, when the computer 4 receives the email message, the look-up procedure starts. It is contemplated that the user of the computer 4 can define the specifics of the event-triggered look-up. For instance, the user can define if a notification of the requested look-up shall occur or if a recording or display of the look-up is desired.

Detailed Description Text (18):
The user of the computer 4 can define how emails from computers whose ID numbers are not stored in the database need to be treated. Depending on user-specified settings of the computer 4, emails from unauthorized/unidentified computers can be, for example, blocked or rejected. For instance, the user can create a contact list in which all authorized users are listed. If the received ID number does not match to the ID number stored for an authorized user from the contact list, the email will be rejected.

Detailed Description Text (19):
These settings, for example, prevent the user from receiving undesired emails from individuals who frequently change their email address or camouflage the return address. These undesired emails cannot be blocked by conventional filters which can be defined in email applications because the filters are typically only sensitive to the field "From:" for the return address.

Detailed Description Text (20):
In addition, the settings prevent the user from receiving unsolicited emails from Internet marketing companies or so-called "spammers." A "spammer" is an individual user or a service which post irrelevant or inappropriate messages to one or more users, send large amounts of unsolicited emails meant to promote a product or service, or intend to crash a program by overrunning a fixed-size buffer with excessively large input data.

Detailed Description Text (21):
Moreover, the computer 4 cannot only block or reject emails from unauthorized users, but also identify if the return email address that appears in the field "From:" is indeed the real email address. For example, the sender of the email could pretend to be an authorized user by changing the email address to one the sender believes the computer 4 accepts. However, because the ID number is included to the received email, the false identity of the sender of the email can be recognized.

Detailed Description Text (39):
FIG. 3 shows an exemplary data format as used in the identification database 32. The identification database 32 includes several fields 32A-32F of predetermined sizes. Each field 32A-32F includes an attribute. In the illustrated embodiment, the ID number is assigned to the field 32A which has a size of 44 bits. The user name and the email address are assigned to the fields 32B, 32D, respectively. The field 32B has a size of 128 bits and the field 32D has a size of 256 bits. The field 32C includes an attribute "activity status" and the field 32E includes an attribute "authentication statues." The field 32F includes an attribute "ISP" defining the Internet service provider. It is

contemplated that the identification database 32 can include additional fields, such as for the IP address, geographical data and other user information.

Detailed Description Text (40):
In one embodiment, only the email address and the ID number are indexed. As is known in the art, an index is a sequence of (key pointer) pairs where each pointer points to a record in the database that contains the key value in a particular field. The index is sorted on the key values to allow rapid searching for a particular key value. In one embodiment, the index can be "inverted" in the sense that the key value is used to find the record rather than the other way round. For databases in which the records may be searched based on more than one field, multiple indices may be created that are sorted on those keys.

Detailed Description Text (42):
The client module 28 prompts the user to input the email address. The user inputs the email address under which the user can receive emails. During a subroutine in state 202, the client module 28 retrieves the ID number from the processor and prepares a message to be sent to the server 26. The client module 28 includes as a default setting, the IP address of the server 26. In addition, the client module 28 may have a list of additional appropriate servers connected to the Internet 24.

Detailed Description Text (44):
Upon connection to the, Internet service provider, the procedure proceeds along the YES branch to state 208. In state 208, the client module 28 (e.g., via SMTP) initiates that the prepared message is sent to the server 26. The message includes the ID number, the user's email address and the IP address. It is contemplated that additional information can be added depending on the data format used, as described below with reference to FIG. 5.

Detailed Description Text (52):
In one example, the users of the computers 20, 22 have both registered with the server 26 through the procedure illustrated in FIG. 4. In addition, the computers 20, 22 defined contact lists so that the computers 20, 22 accept only emails from authorized computers.

Detailed Description Text (56):
Proceeding to state 304, the user of the computer 20, or any other registered computer, can request a look-up of an email address from the server 26. Here, the user requests a look-up of the email address of the user of the computer 22. The user of the computer 20 prepares a message (email) to the server requesting the look-up of the email address included in the message. The message is sent over the Internet 24 to the server 26.

Detailed Description Text (57):
Proceeding to state 306, the server 26 receives the message from the Internet 24 ad initiates processing the message. The processing includes starting a module to look-up the email address in the identification database 32. The subroutine uses known methods to access and retrieve data from a database. The subroutine extracts the look-up email from the received message and checks if the identification database 32 includes a matching entry.

Detailed Description Text (58):
Proceeding to state 308, the server 26 generates a second message that is a response to the first message received from the computer 20. If the look-up did not result in a matching address, the second message informs the user of the computer 20 that no matching entry has been found. If, however, the look-up was successful, the second message includes an authenticated email address, authenticated because the email address is correlated to the unique ID number. In addition, the second message can include data indicating, for example, if the computer 22 is currently registered as active, i.e., if the user of the computer 22 is online at the moment.

Detailed Description Text (59):
Proceeding to state 310, the computer 20 receives the second message and extracts the authenticated email address of the computer 22. As in a conventional email application, the user of the computer 20 can read the email upon receipt or at a later time.

Detailed Description Text (60):
Proceeding to state 312, the user of the computer 20 can directly communicate with the user of the computer 22 using the authentic email address. To communicate, the user of the computer 20 has several options. The user can send an email to the user of the

computer 22 that will be recognized as coming from a known contact. Alternatively, the user can connect directly to the computer 22 to initiate an online conferencing connection, such as a chat connection, a video conference, or a voice connection, if the user of the computer 22 is currently online or available. The procedure ends at state 314.

Detailed Description Text (61):
The described look-up via email address is typically the only way for users to find one another. This makes the system a closed system and attractive to users who do not want their information published. In particular, the system provides improved security and confidentiality for transactions that involve financial or personal data.

Detailed Description Text (67):
As soon as the user USER-1 is online, the client module 50 API (SDK) automatically sends a message to the server 26, as indicated through a connection line L1. The message includes the ID number. The message may also include, but is not limited to, the IP address and email address as described above. The directory module 74 receives and processes the message and initiates an update of the identification database 32. The user USER-1 is then stored as an active user.

Detailed Description Text (68):
If the user USER-i wants to communicate with the Internet service provider ISP-1, the user USER-1 requests a look-up of the email address of the Internet service provider ISP-1. The server 26 executes this look-up request and generates a response if the requested email address matches one of the stored and authenticated email addresses. The generated response includes the IP address of the Internet service provider ISP-1. The response sent to the user USER-1 is indicated through a connection line L2. Using the IP address, the user USER-1 can then directly connect to the Internet service provider ISP-1.

Detailed Description Text (70):
If the user USER-2 requests a look-up of the email address of the user USER-3, the response includes the IP address of the computer 44 of the user USER-3. The user USER-2 can then directly connect to the user USER-3 to send an email, to chat, to have a video conference, or the like. The connection between the computers 42, 44 is indicated as connection line L8.

Detailed Description Text (71):
It is contemplated that the user USER-2 can look-up a variety of email addresses. A general connection with a computer connected to the Internet 24 is indicated through a connection line L9. Correspondingly, the user USER-3 can connect to the Internet service provider ISP-2 via the Internet 24, as indicated through a connection line L1 . Alternatively, the computer 22 and the service computer can be connected through the communications link 60, as described above.

Detailed Description Text (76):
In this example, the web computer 80 and the client computer 84 have registered with the server 26 according to the registration procedure illustrated in FIG. 4. Using a communications link C1, the user of the client computer 84 requests a look-up of the email address of the Internet shop. The server 26 performs the look-up in its database 92 and returns an authenticated email address if the look-up email address matches to an entry correlated to the ID number in the database 92.

Detailed Description Text (77):
The user of the client computer 84 can then establish a direct communications link C2 with the web computer 80 using the authenticated email address. This assures the user of the client computer 84 that the communication occurs directly with the Internet shop when the user places an order with the Internet shop. In some cases, the Internet shop requires that the order include consumer-specific data such as name, address and the number of the credit card.

Detailed Description Text (78):
Before the Internet shop confirms the order via a communications link C3, the Internet shop can request a look-up of the client's email address to ensure that the data of the order is correct. The look-up request and the resulting response occur via communications links C4, C5, respectively.

Detailed Description Text (79):
As described above, the ID numbers are unique within the identification database 32 as

well as within the Internet 24. In contrast, user names and email addresses, for example, can appear more than once within continuously growing global Internet. Because of this, there may be two users that claim to have the same email address. If such a collision occurs on a lookup, both users will be returned from the query. The identification database 32 permits users to look up other users only by email address and not by the ID number. However, the index to the ID number is there, because the contact list may need to look up a specific ID number.

CLAIMS:

1. A method of maintaining a user identification database that indicates when users are in communication with a network, the method comprising the acts of:

associating in a computer accessible storage medium electronic mail addresses, processor-embedded identifiers and status information;

receiving a first electronic message from a first computer, the first electronic message containing an electronic mail address and a copy of the processor embedded identifier existing in the first computer;

using the first electronic mail address to access the corresponding processor-embedded identifier stored in the storage medium;

comparing the processor-embedded identifier from the first computer with the processor-embedded identifiers of the storage medium;

modifying the status information in the storage medium to indicate that the first electronic mail address is authentic when the processor-embedded identifier from the first computer matches a processor-embedded identifier of storage medium;

receiving a second electronic message from a second computer, the second electronic message requesting authentication of the first electronic mail address;

comparing the first electronic mail address with the electronic mail addresses stored in the storage medium; and

sending a third message to the second computer that indicates whether the first electronic mail address is authentic.

2. The method of claim 1, further comprising the acts of:

obtaining the status information that corresponds to the first electronic mail address; and

including the status information to the third message.

3. The method of claim 1, further comprising the act of using the authenticated first electronic mail address to establish a communications link between the first and second computers.

5. The method of claim 1, wherein the act of receiving the second electronic mail includes indicating the second computer as active in the storage medium.

6. The method of claim; 1, wherein the act of associating electronic mail addresses includes registering the first and second computers in a computer accessible database.

7. The method of claim 6, wherein the act of registering includes storing each processor-embedded identifier in the database together with the electronic mail address of the registering computer.

WEST

Generate Collection Print

L4: Entry 7 of 8 File: USPT Mar 6, 2001

DOCUMENT-IDENTIFIER: US 6199102 B1
TITLE: Method and system for filtering electronic messages

Brief Summary Text (4):
By taking advantage of the growing popularity of the Internet, a user can send messages to a receiver located virtually anywhere in the world. There are a number of advantages to sending messages via electronic mail (email) rather than through the U.S. Postal Service. By using email, it may take only seconds for the sender's message to be received by a receiver on the other side of the world. The receiver can read the sender's text immediately on the screen, respond to it right away, save it for later, print it, or quickly forward it to another receiver. Messages a user receives can be organized into convenient electronic folders and saved for as long as the user wishes without taking up office space. Due to these advantages, email has become many people's principal means of communicating with the world.

Brief Summary Text (5):
A further function of electronic mail allows a user to create electronic mailing lists for sending notices to hundreds or even thousands of people at once. Due to the ease of sending electronic mail to a very large number of people, the number of mass mailings for unsolicited advertising has risen dramatically. Unlike advertisements through the U.S. Postal Service, it is not necessarily clear to the user that the message is for advertising purposes until the user opens and reads the message. Thus, the target of the unsolicited electronic commercial message must typically open the message, read a portion of it, then, after determining it to be unwanted "junk", delete it. A user receiving several of these commercial messages can easily expend valuable time, resources and mental aggravation.

Brief Summary Text (6):
Companies and individuals in the business of mass commercial emailing have shown a reluctance to stop their practice or refrain from contacting recipients who do not want to receive promotions. This business, like traditional junk mail, is profitable. Since the cost of sending emails is so low, a junk e-mailer (commonly referred to as a "spammer") benefits by contacting the largest and broadest group of recipients as possible--more recipients means more people who might be interested in the message--even if it also means a larger group of outraged recipients.

Brief Summary Text (7):
Members of the electronic community have tried to create numerous roadblocks to stop spamming--some electronic, some legal, and some with a business focus. Unfortunately, the junk email sending community has generally adapted to and overcome each one.

Brief Summary Text (8):
An attempt to request the advertiser to stop soliciting the user is typically severely hindered since it is common practice for advertisers to either not provide a reply address or to make up a false reply address. Since some email systems (the Internet in particular) do not require a valid reply address nor a valid sender name, most ads can be repeatedly sent to thousands of people without giving the recipients a convenient method to request that they be taken off the advertiser's list. Spammers who do provide valid reply information are often unresponsive to requests to desist. Accordingly, thousands of email users must suffer through a barrage of unwanted email advertisements which typically must be opened in order to determine that it is an (unwanted) advertisement. In lieu of a valid email reply address, some of these unsolicited commercial messages will give a non toll-free number. In order to contact the advertiser, the user must pay for a phone call which may be long distance.

Detailed Description Text (3):

Although the present invention is described in terms of a system which receives e-mail, it is to be understood that email is merely an example in which the present invention can be applied. For instance, the present invention can also be applied to electronic messages in video form wherein unsolicited commercial messages can be sent via video.

Detailed Description Text (5):
Conventional message filtering involves the use of a mail filter in an email recipient's local email system. Such a filter typically sorts incoming email for the recipient into categories determined by the recipient. The filter typically simply scans elements of each email message as it reaches the recipient and determines what category it should be placed in depending on certain criteria. One category is "discard". Messages which the filter places in the discard category are automatically discarded, but in practice the direct deletion of messages via a filter is extremely risky. A perfect filter would catch and dispose of all junk messages and retain all non-junk messages, but such a filter has yet to be demonstrated. This imperfection is primarily caused by the inability of most filters to determine what constitutes "junk email". For this reason, most filter designs take a different approach and move suspected junk messages to a temporary or miscellaneous holding category for review by the recipient before deletion. Invariably, desired messages are accidentally marked for deletion and junk messages slip through the filter. The user must typically manually correct these mistakes.

Detailed Description Text (6):
Conventional filters have had varying degrees of intelligence; some have simply worked with lists of mail addresses and have sorted messages according to the source of the message; others have used keywords provided by the recipient to sort; with others, finally, the filter observes how the recipient sorts his email and is then able to sort in a similar fashion (usually by utilizing a combination of the two previous methods--source lists or keyword/content searches).

Detailed Description Text (7):
Each of the message filtering methods has weaknesses that can and typically are exploited by junk email senders. The source list method requires a message sender to be on a list (either an acceptance or blocking list) in order to permit the filter to take action. A message from an unknown sender (frequently a solicitor) cannot be discarded because it might be from, for example, a new business contact or a long-lost friend. By constantly using new sender addresses, a solicitor can assure that junk messages will pass through a source list filter and come to rest in a temporary or miscellaneous category reserved for messages that are not actionable. Messages in this category must typically, at least briefly, be scanned by the recipient--a successful defeat of the filtering mechanism. The second method--keyword/content searching--has the potential of discarding wanted, as well as unwanted, messages. Any keyword or phrase search (with the intention of identifying and dealing with particular message subject matters) will eventually discard a bona fide message that appears to be "junk" in nature. For example, searching and discarding all messages with the words "make money" in them might get rid of some junk messages, but it will also eventually discard a desired message such as a new business idea from a brother or sister that happens to use the same words or word patterns. Again, the flaws in this approach force most implementations to place incoming messages in a temporary holding category. And again the messages in this category will, at least briefly, be scanned by the recipient a success for the solicitor.

Detailed Description Text (8):
It should be noted that there are some message filtering techniques that rely upon the sender to indicate the subject or target audience of their message. The recipient's filter can then look for and operate on these messages with the recipients best interests in mind. These can work successfully, for example, in a corporate environment where both the senders and recipients have a working relationship and an active interest in effectively using each other's time and communication resources wisely. For example, all incoming resumes might be marked as high priority for a human resources manager, but the sender would have to indicate, via a predetermined method, that the content of the message was a resume. The human resource recipient could then configure their email processing system to categorize and correctly handle these resumes. These techniques are ineffective, however, when the sender is not cooperative and uninterested in having their messages intercepted and screened by this mechanism. Most junk email senders on the Internet fall into this category. The business of sending junk email is typically profitable, legal, and effective. There is no incentive for such an individual or company to actively make it easier for recipients to discard or ignore their messages. Indeed, most spammers make money by emailing more individuals,

not less. Any technique, therefore, that attempts to stop this flow of unwelcome messages, can not rely on the cooperation of the message senders. In fact, this group has shown the exact opposite tendency in actively pursuing means of circumventing any and all filtering techniques.

Detailed Description Text (9):
Even if these filtering techniques provided a reasonable means of relief from the junk email onslaught, they still suffer from the need to be actively maintained. For example, source lists must continually be updated as solicitors use new sender addresses. And keyword lists must be continually modified as solicitors send widely varying and extremely creative messages which resemble legitimate communications. In either case, the temporary holding category must typically be reviewed for mistakes and the filtering apparatus must be maintained. Junk email usually causes frustration because of the time wasted in dealing with it. The use of conventional message filters has simply traded one means of spending time with another with no net gain.

Detailed Description Text (11):
A feature of the present invention is the checking of incoming messages to verify that they include valid sender information. Any message which does not contain a valid sender address is assumed to be a junk email communication and is dealt with appropriately (generally deleted).

Detailed Description Text (13):
Another feature of the present invention is the checking of incoming messages to verify that each message is properly addressed to the user (the recipient). For example, a message which is not addressed to the recipient will be assumed to be a junk email communication and dealt with appropriately (generally deleted).

Detailed Description Text (14):
When determining whether an incoming message is actually addressed to the recipient, the method according to the present invention will consider various appropriate recipient designations for the messaging system being used. In other words, it is possible that the recipient will receive a valid message that is not directly addressed to him. Instead, he might be a CC (carbon copy) recipient, or perhaps a BCC (blind carbon copy) recipient. There may be other possible message recipient designations. As long as the invention user's address is present on at least one of these recipient designations the message is considered valid. If the user's address is absent from all of these recipient groups the incoming message is considered junk email.

Detailed Description Text (15):
Yet another feature of the invention is that it prompts unrecognized email senders, for example, by returning their message and asking them a predetermined question or one of a set of predetermined questions:

Detailed Description Text (23):
Preferably a block of text is added to the beginning of an incoming email message from an unknown sender. The sender's original message is preferably preserved. This block of text is referred to as a Challenge and contains, among other elements, a prompt, such as a question similar to those above. It also contains an answer blank area where the sender is requested to place their response to the prompt. After adding the Challenge text to the original message, thereby creating a modified message, the modified message, is returned to the sender. The sender must answer the Challenge (which includes the prompt) and send it back to the recipient. Upon receiving a completed Challenge, the answers are checked for validity. If the answers are correct, the message is forwarded to the recipient. Otherwise the message is blocked and discarded.

Detailed Description Text (25):
If, on the other hand, they provide accurate sender information they will then be inundated by Challenges from users of this invention, in addition to vast quantities of undeliverable returned messages and other detritus. In order to reach users of this invention, the spammer must staff relatively large banks of people to answer these Challenges (because a computer cannot). The staff to sort through the incoming mess of messages and manually answer Challenges will cost money and hurt the profitability of the junk email business. Many in the business would likely choose to avoid this step by either not including a sender address or ignoring all returned email--in either case their unwanted transmissions do not reach a user of the method and system according to the present invention.

Detailed Description Text (27):

FIG. 2 is a block diagram of networking system with which the present invention can work. The Internet system 50 is shown to include mail servers 52a-52c which utilize the standard protocol of Simple Mail Transfer Protocol (SMTP). A message 54 can be sent via one of the SMTP servers, such as the server 52a. The message may be passed through several servers before reaching its final destination, in this example, the server 52c. Once the message is received by the destination receiver 52c, then it is typically sent to a mailbox 56, such as a Post Office Protocol box (POP) or Internet Message Access Protocol box (IMAP) where it is held pending retrieval by an Email Client Program 60. During message retrieval, the message can be filtered through the Message Filter Program 58. Note that the Message Filter 58 according to the present invention can be located in various locations including between the Mailbox 56 and the user's Email Client Program 60; as part of mailbox servers such as Mailbox 56, or in the Email Client Program 60 which actually processes the user's messages. In the example shown in FIG. 2, the Message Filter 58 according to the present invention is shown to be located between the Mailbox 56 and the Email Client Program 60. In the following figure (FIG. 3), the message filter is shown incorporated into the Email Client Program.

Detailed Description Text (28):
FIG. 3 is an example of a networking system in which the present invention can operate. Filtering Enabled Email Client Program 100 is shown communicating with a Network 110 that facilitates communication among other members of the network. Filtering Enabled Email Client Program (FEECP) 100 is resident and actively run on a computer system illustrated in FIG. 1 which also provides the network connection.

Detailed Description Text (29):
Filtering Enabled Email Client Program 100 communicates with Network 110 which connects a number of Users 101a-101c. Network 110 may be a network such as the Internet or a commercial email network, or it may be a 101c an email system which communicates internally between users of a single computer system. Users 101a-101c are interconnected to this network by one or more links 103 over which each User 101 may send and receive electronic messages (email).

Detailed Description Text (30):
The Network 110 connects any number of computer systems 101a-101c, each being able to facilitate at least one user. Each user attaches to and interacts with the Network 110 (and other Users 101) by means of a device, generally a computer, that sends, receives, interprets, and acts upon the signals transmitted across the network. Each user 101, therefore represents not only an individual, but also the computing devices and email client programs that allow them to communicate over network 110. These computers may vary greatly in their construction and manner of use. They may contain different configurations of logic processing software and may have different capabilities (for example, some may have email client mail filters like this invention and some may not.) For the sake of this discussion, each will have, at the minimum, rudimentary capabilities to compose, send, receive, and manipulate electronic messages over network 110 by way of an email client program.

Detailed Description Text (31):
Filtering Enable Email Client Program 100 (and the user(s) that use it) has the same characteristics and capabilities as normal Users 101, but also implements the various part of the message filtering system of the present invention. The system and method according to the present invention allows the user to reduce the amount of junk email received from the network (and hence other users). There may be multiple users on the network that implement a Filtering Enabled Email Client Program 100, but this discussion will focus on only one such user for the sake of clarity.

Detailed Description Text (32):
Filtering Enabled Email Client Program (FEECP) 100

Detailed Description Text (37):
Acceptance List 105 contains zero or more email addresses or address patterns in a list--maintained on a non-volatile storage device--that can be retrieved, edited and saved.

Detailed Description Text (38):
The Acceptance List 105 contains email sender addresses (and therefore email senders) that are permitted to communicate unimpeded with the recipient. Any incoming message with a sender address contained in or matching a pattern on this Acceptance List will be permitted to reach the recipient.

Detailed Description Text (41):
The Blocking List 115, like the Acceptance List 105, also contains zero or more email address or address patterns in a list--also maintained on a non-volatile storage device--that can be retrieved, edited and saved. This list, however, performs the opposite function--any message with a sender address contained in or matching a pattern on the Blocking List 115 is filtered and blocked from reaching the recipient.

Detailed Description Text (44):
If an email solicitor correctly answers a Challenge and reaches the recipient against his wishes, the recipient (i.e.--the user of this invention) can manually add the sender's address to Blocking List 115. (The manual entry of blocking addresses would occur through the use of the User Interface 109.) From that point forward, any incoming messages from that sender would be filtered and discarded.

Detailed Description Text (47):
The prompts (and answers) stored in 106 could be entered as part of a pre-built, or commercial release of a method and system according to the present invention. This practice, however, would allow a junk email sender to procure the fixed prompt list and create an automated program capable of recognizing and answering the limited prompts therein. Instead, a feature of the present invention is that each user himself enters prompts (and answers) in to the Repository 106 (by using User Interface 109.) By having each user compose and enter their own prompts, the possible permutations are limited only by human imagination. In such a case, it would be extremely difficult, if at all possible, to automate the answering of Challenges because the variety of possible prompts would be too great.

Detailed Description Text (58):
The General Notice preferably is the first thing that a sender reads when their message is returned (with the included Challenge). It can be anything the user wants. It is suggested, however, that this information describe the reason the sender's mail has been returned (i.e. predicated upon a proper response to a Challenge) and the process that the sender must complete in order to reach the recipient (instructions on completing the Challenge prompt and Legal Notice). In addition, it might be advisable to include an alternate contact means such as an address or fax number where the recipient can be reached. This would be valuable if the sender, for some reason such as technical difficulties, cultural differences, or language differences, had trouble correctly responding to the Challenge. In such a situation, they could use the auxiliary contact means to reach the recipient. It would be important, however, to cover the auxiliary contact means in the Legal Notice as well as the recipient's email address.

Detailed Description Text (61):
This Legal Notice, like the Challenge prompt from 106, must also be answered correctly by the sender in order for the Challenge to be valid. Unlike the prompt from 106, however, the correct answer to the Legal Notice is always an affirmation. For example, after reading the Legal Notice as part of the Challenge, the user would be prompted to type the word "AGREE" in a designated blank. The Legal Notice should specify that typing "AGREE" signals an understanding and agreement to the terms of the notice. If the sender does not agree to the Legal Notice, their email communication will be filtered and blocked upon being returned to Mail Processor 104.

Detailed Description Text (63):
Email messages resident in the Filtering Enabled Email Client Program 100 are stored in categorized Message Folders 108(a . . . n). These Message Folders (and the messages contained within them) are stored on non-volatile storage and can be retrieved, created, manipulated, and stored through the use of User Interface 109. The messages contained (and to be contained) within the Message Folders can also be manipulated by the Mail Processor 104 during the process outlined in FIG. 7.

Detailed Description Text (65):
In addition to user created message folders, this system preferably has two special-purpose default message folders--"New" and "Deleted". Mail Processor 104 places all incoming email messages that are not filtered and not blocked into the "New" folder. Mail Processor 104 places all incoming email messages that are filtered and blocked into the "Deleted" folder. The filtering and blocking process is outlined in FIG. 7.

Detailed Description Text (67):
Messages that are deleted (either by the Mail Processor 104 or manually by the user)

are placed in the "Deleted" system message folder. By placing a message in this folder, it is not actually deleted. Essentially is becomes marked for deletion which will occur at some future event. This temporary holding of deleted messages allows the user to correct an accidental deletion or recover a wrongly filtered incoming message. To do so, the user simply moves the desired message out of the "Deleted" folder into another message folder. The permanent deletion of items in the "Deleted" message folder can be configured by the user to occur after various events including manually, after a time interval, and after a certain amount of "Deleted" email has been accumulated.

Detailed Description Text (69):
Every significant action that the Filtering Enabled Email Client Program 100 performs is preferably, at the option of the user, logged to the system Log File 114. Each action would be noted in this log along with specific information to make the entry useful. For example, an incoming message from "John_Smith@aol.com" whose address is on a Blocking List might cause a log file entry such as:

Detailed Description Text (74):
Each of the Filtering Enabled Email Client Program 100 components interacts with the user via the User Interface 109. Some examples of what the user can do:

Detailed Description Text (101):
FIG. 4 is another example of a networking system in which the present invention can operate. In this example, the Filtering Enabled Email Client Program 100 from FIG. 3 has been split into two separate programs--Message Filtering Program 100a' and Email Client Program 100b'. As before, both of these programs are resident and run on an appropriate computer system, but the systems can be separate (i.e. two computers, one running each component).

Detailed Description Text (102):
The Message Filtering Program 100a' contains all message filtering components of the present invention. The Email Client Program 100b' consists of a normal email client and does not have the ability to filter incoming messages according to the present invention. During normal operation of FIG. 4, the Email Client Program 100b' will retrieve messages through the Message Filtering Program 100a'. While messages are being retrieved, the Message Filtering Program 100a' will challenge, block and delete all appropriate message according to the flow diagram in FIG. 4. Incoming messages which are not blocked are allowed to pass through to the Email Client Program 100b'. And, as before, outgoing messages are transmitted unimpeded.

Detailed Description Text (103):
In this figure, both programs have a User Interface (109a' and 109b'). This allows the use and configuration of each program separately. Each program also has a Mail Processor (104a' and 104b'). In this figure, Mail Processor 104b' only has the ability to send and receive email. Mail Processor 104a', however, retains the ability to analyze and filter incoming messages as well as also having the ability to send and receive mail (which come from and go to the Email Client Program).

Detailed Description Text (105):
FIG. 5 shows an example Internet email message 201. This message is composed of a message header 202 and message body 203. The message body 203 contains the substance of the message and is the part which is intended for the message recipient. It will typically include text, but may also include files, pictures, sound, video, etc. depending on the particular messaging system being used. The message header 202 contains information about the message and the message body ("meta" data). This information usually includes the message sender, the message recipient, the subject of the message, the length of the message, the time the message was composed, etc. Many other pieces of information and combinations are possible.

Detailed Description Text (106):
FIG. 6 shows the composition of a Challenge 301. The Challenge is a section of text which is preferably inserted in the body 203 of an email message 201. Once inserted, this newly modified message is returned to the sender. The challenge consists of a Header 305, General Notice 302, Legal Notice 303 and Prompt 304.

Detailed Description Text (117):
When composing the Challenge 301, the Mail Processor 104 will insert a blank, affirmation entry field 303b into the text after the Legal Notice 303a. This field, like the header token, will be delimited by certain predetermined characters that are chosen because of their unlikely probability of occurring in an email message unless

placed there on purpose. For example, the affirmation blank 303b could be constructed as such:

Detailed Description Text (119):
The choice of three pound signs and then two greater than symbols (with the opposite at the end of the entry blank) would be extremely unlike to occur in a normal email message unless placed there on purpose.

Detailed Description Text (123):
Rather than "agree", another word or phrase or even a varying range of affirmative responses can be used. This could be set up similar to the Challenge prompt such that a different affirmative response is required for each Challenge. By doing this, it would become difficult for an email solicitor to automate the response to the Legal Notice.

Detailed Description Text (126):
As in the case of the Legal Notice Affirmation Blank 303b, the Mail Processor 104 will insert a blank entry field 304b into the Challenge 301 after the prompt. The sender will be instructed to answer the prompt and enter their response in the Answer Blank 304b. As also in the previous case (303b), the Answer Blank 304b will be delimited by predetermined characters that have a low probability of occurring naturally in an email message. For example, the Answer Blank 304b could be constructed as:

Detailed Description Text (152):
Any message which is not properly addressed to the recipient will be assumed to be a junk email communication and dealt with appropriately (typically deleted). The user can configure various parameters which determine whether an incoming message is "properly" addressed to the recipient depending on such conditions as whether the recipient's email address is present in the message's recipient fields, which recipient field(s) the recipient's address appears in, how many secondary recipient addresses (those not belonging to the user) are present in the message's recipient fields, and which message recipient fields contain those secondary addresses.

Detailed Description Text (153):
On the Internet, for example, it is possible for a user to receive a message which is not addressed to them in any way. In other words, such a message does not contain the user's email address (or name) in any of the message's recipient fields. Such fields may include TO (which generally indicates the main message recipients), CC (which generally indicates carbon copy recipients), or perhaps BCC (which generally indicates blind carbon copy recipients). There may be other possible message recipient fields. It is an option of the present invention to identify such incoming messages as junk email and deal with them appropriately.

Detailed Description Text (154):
On the Internet, for example, it is possible for a user to receive a message which is not solely addressed to them. This condition would exist if the message's recipient fields contained the user's address and also contained addresses of other (secondary) recipients. It is an option of the present invention to identify as junk email any incoming message which is not solely addressed to the recipient. It is also an option of the present invention to identify as junk email any incoming message which is not solely addressed to the recipient when the number of secondary recipients of the message exceeds a predetermined threshold (10 for example).

Detailed Description Text (156):
(1) Accept incoming email regardless of message's recipients.

Detailed Description Text (157):
(2) Accept incoming email only if I am one of the message's recipients.

Detailed Description Text (158):
(3) Accept incoming email only if I am the sole message recipient (no other recipients in the message's recipient fields).

Detailed Description Text (159):
(4) Accept incoming email only if I am one of the message's recipients and there are no more than N other message recipients.

Detailed Description Text (160):
(5) Accept incoming email only if I am the sole primary message recipient (i.e. my address is the only recipient address in the TO: recipient field).

Detailed Description Text (161):
(6) Accept incoming email only if I am a primary message recipient (i.e. my address is in the TO: recipient field) and there are no more than N other primary recipients.

Detailed Description Text (176):
If the incoming message does not contain a Challenge then the message is from a new, unrecognized sender that has never correctly answered a Challenge and/or never been placed on the Blocking List 115. In this situation, the message sender will be Challenged in an attempt to exclude junk email (which this message could be).

Detailed Description Text (178):
Various heuristics can be applied to an email address to determine if it is valid. These heuristics will vary depending on the messaging standards of the medium of transmission. On the Internet, for example, an email address must contain the symbol `@`. An email address without this symbol is invalid.

Detailed Description Text (188):
If both the Prompt 304b and Legal Notice responses 303b are valid the message is accepted and placed in the "New" Message Folder 108x. In addition, the sender's address is entered into the Acceptance List 105. This assures that all future emails from this sender are accepted without the issuing of a Challenge (unless the Acceptance List 105 is cleared manually by the user, or unless the sender's address is subsequently added to the Blocking List 115).

Detailed Description Text (190):
A useful feature, anticipated, but not implemented in the preferred embodiment would involve a modification of the Acceptance List 105. Recall that this list includes addresses of all sender's whose email messages may pass through, unimpeded, to the recipient. By adding extra information to the Acceptance List, it would be possible to automatically categorize all incoming messages. For example, an entry in the Acceptance List allowing a grandmother to communicate with the recipient might consist of:

Detailed Description Text (192):
By adding an additional piece of information to this list entry, we could automatically send all of grandma's email messages to the "Grandma" Message Folder 108x (assuming one exists). This modified Acceptance List entry might look like: